Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations   1. Thesis and Dissertation Collection, all items

1987-09

Ship-shore packet switched communications system and an application in Hellenic Navy

Agapiou, Evagelos S.

http://hdl.handle.net/10945/22473

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

SHIP-SHORE
PACKET SWITCHED COMMUNICATIONS SYSTEM
AND AN APPLICATION IN HELLENIC NAVY

by

Evagelos S. Agapiou

September 1987

Thesis Advisor: Thomas J. Brown

Approved for public release; distribution unlimited.

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release, distribution unlimited
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	

4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)

6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b OFFICE SYMBOL (If applicable) 62	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000		7b ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000

8a NAME OF FUNDING/SPONSORING ORGANIZATION	8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (City, State, and ZIP Code)		10 SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO	PROJECT NO	TASK NO	WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification) SHIP-SHORE PACKET SWITCHED COMMUNICATIONS SYSTEM AND AN APPLICATION IN HELLENIC NAVY (UNCLASSIFIED)

12 PERSONAL AUTHOR(S)
Agapiou, Evagelos S.

13a TYPE OF REPORT Master's Thesis	13b TIME COVERED FROM _____ TO _____	14 DATE OF REPORT (Year, Month, Day) 1987 September	15 PAGE COUNT 180

16 SUPPLEMENTARY NOTATION

COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Communications System Engineering, Ship-shore, HF Communications, Packet Switching

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

Computer to computer communications have advanced rapidly in the last years. High Frequency (HF) communications systems have not kept pace with these advances and have generally not been considered suitable for high speed data communications.

This thesis presents an architecture for ship-shore sea service communications. It starts with the problems that make sea service communications different from conventional systems (Local Area Networks, LANs). Then, these problems are integrated into a complete system by using the ISO reference model. The first three layers of the ISO reference model, physical, data link, and network layers are examined in reference to these problems.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION Unclassified
22a NAME OF RESPONSIBLE INDIVIDUAL Thomas J. Brown	22b TELEPHONE (Include Area Code) 408-646-2772 22c OFFICE SYMBOL 62Bb

DD FORM 1473, 84 MAR   83 APR edition may be used until exhausted   SECURITY CLASSIFICATION OF THIS PAGE
All other editions are obsolete

(19. continued)

An examination concludes that a ship-shore packet switching communications system is applicable in Hellas and its Navy.

Approved for public release; distribution is unlimited.

Ship-Shore Packet Switched Communications System
and an Application into the Hellenic Navy

by

Evagelos S. Agapiou
Commander, Hellenic Navy
B.S., Hellenic Naval Academy, 1971

Submitted in partial fulfillment of the
requirements of the degree of

MASTER OF SCIENCE IN TELECOMMUNICATIONS SYSTEMS MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 1987

ABSTRACT

Computer to computer communications have advanced
rapidly in the last years. High Frequency (HF)
communications systems have not kept pace with these
advances and have generally not been considered suitable for
high speed data communications.

This thesis presents an architecture for ship-shore sea
service communications. It starts with the problems that
make sea service communications different from conventional
systems (Local Area Networks, LANs). Then, these problems
are intergrated into a comlete system by using the ISO
reference model. The first three layers of the ISO reference
model, physical, data link, and network layers are examined
in reference to these problems.

An examination concludes that a ship-shore packet
switching communications system is applicable in Hellas and
its Navy.

TABLE OF CONTENTS

5

8

9

LIST OF TABLES

10

LIST OF FIGURES

11

12

ACKNOWLEDGMENTS

No work such as a thesis is created in a vacuum. The efforts and cooperation of many individuals have been immeasurable support to me to switch express my thanks to Professor Major Tom Brown for his guidance and especially his patience throughout the course of this thesis. Also, my thanks to Professor Richard A. Mcgonical as second reader of the thesis and for his excellent job as International Education Coordinator.

And last, but certainly not least, to my wife Pelagia and my sons Stavros and Panagiotis, whose constant support and love created a happy atmosphere and made it all possible.

I. INTRODUCTION

A. THE EXTERNAL ENVIRONMENT

From the beginning of human creation, a major objective has been to develop a means to communicate with each other. Primitive forms of communication include pictures, signals by hands or grimaces, smoke signals, nineteenth century telegraphy, and certainly the current computer-communicatons revolution.

The 1970s and early 1980s was a merger of the fields of computer discipline and data communications that radically changed the technology, products, and companies of the now combined computer-communications industry. In recent years we have been experiencing a technological revolution in which it is difficult to separate processing and communications. The trend is increasing due to the constant improvement in computer processing speed and storage capacity, and to reduction in price and size. There are also been an increasing of packet switching techniques that are moving from the laboratory to industry.

All these developments make it increasingly attractive to use programmable computers to control communications networks and process the information transmitted through them. This allows the integration of conventional communications with computer networks and distributed

14

systems, while using the same means of transmission, and thus represents a more efficient use of the communication channels. This condition creates a requirement for new transmission techniques that can accommodate the requirements of higher data rates, as well as procedures to handle larger volumes of data.

A great deal of study and organization has gone into the discipline of computer to computer communications, culminating in an efficient shoreside communications systems. A useful reference model has been developed by the International Standard Organization (ISO), which decomposes the greater problem into parts that can be solved individually.

Alas, military communication, especially ship-shore systems, have lagged behind the technological and academic developments in packet switching. There are many cautions that can explain this lag. Most important are:

   * A large amount of investment has been spent and now it
     is a little bit difficult to change.

   * The HF radio communications technology has not kept
     pace with the advances in high speed data communi-
     cations.

   * The standards that have evolved to support conventi-
     onal communications networks are deficient when ap-
     plied to sea service communications.

B. PROBLEMS

The main purpose of this thesis is to develop an architectural design for link termination equipment specific

15

to the High Frequency (HF) environment which is used for sea service communications. This thesis examines and applies the advances in digital technology to the High Frequency (HF) problem. Of primary interest are the issues of link integration, network access, and error control at the network and logical link layers in the HF system.

In order to accomplish this design, the immediate primary problems are examined. There are four immediate primary problems that make sea service communications different from conventional systems. There are two qualitative problems [Ref. 1]:

* The physical links that are used in sea service communications are one way only. This is in contrast to conventional networks which are built on the assumption of full duplex communication. Also a ship may require greater capacity than is offered by a single channel. In this case, the ability to harness several channels together is required.

* All users cannot hear each other. This is the case that complicates the network access problem, especially in light of the constricted bandwidth.

and two quantitative problems:

* A constricted bandwidth. A High Frequency (HF) narrowband channel will carry 1000 (1K) to 10,000 (10K) baud. This range is about three orders of magnitude less than the capacity of current conventional Local Area Networks (LANs).

* High noise level. In the case of High Frequency (HF) communications one bit error in 10^2 or 10^3 is not uncommon. This is roughly three orders of magnitude worse than that observed in conventional Local Area Networks (LANs).

In sea service communications there are some additional characteristics such as synchronous communications require-

ments and frequency has entirely lost imposed by the medium. These characteristics can be worsened even further in a combat situation due to enemy jamming.

C. A FIRST CONDUCT WITH THE PROBLEMS

These four problems, mentioned above, are dealt with in three major parts and are first examined in this chapter [Ref. 1].

1. Lack of Full Duplex Capacity

Many sea service communications are organized as fleet broadcasts and, therefore, they are not duplex, nor can duplicity be faked by reversing the channel quickly. This event must be accepted for Emission Control (EMCON), as well as physical ones. But, the lack of full duplex capability invalidates the conceptual communications model that underlies the CCITT and IEEE standards because they are predicated on the capability to support full duplex communications at the physical level.

The second aspect of this problem is the requirement to provide a user with more than one link when the user requires greater capacity than is available on a single channel. This is the case of downward multiplexing and internetworking.

The solution to this problem is to recast the reference model. The best rearrangement is to transfer the packet acknowledgement from the logical link layer to the

17

network layer. A proposed network protocol is presented to implement this solution. With the exception of the network packet acknowledgement, all the relevant problems become readily apparent. Indeed, the concept of combining each communications band from ELF to EHF in a fully integrated system rather than as separate systems becomes clear.

2. Network Access

The second part of the problem is that all users cannot hear each other. This means that there must be a device which determines who talks when on a network. In broadcast communications (long haul HF environment), all subscribers must hear the network control station (communication center), but no assumptions can be made about subscribers hearing each other. The ability of all subscribers to hear each other is an assumption in collision avoidance, collision detection, and token systems.

There are many feasible solutions to this problem, and all are dependent on centralized reservation systems.

3. Presence of Noise

Our purpose is to use efficiently the available bandwidth. There are many modes to increase the throughput, and the data rate of a channel. For example, data compression techniques can improve the throughput and higher performance modems can increase the data rate range from the current 75 to somewhere from 1-10K, in a channel.

But an increased data rate is not sufficient. More error control tools are required to face the noise problem. The standard automatic repeat request (ARQ) technique of packet systems is by itself, not sufficient. In this thesis three appropriate tools are implemented in adaptive fashion so that they use bandwidth only as necessary. These error control techniques must be implemented with care because they require bandwidth which is already a scarce commodity in the HF environment.

The solution to this part is the architecture design of the link termination equipment.

D. COMMUNICATION NETWORKS

There are two basic types of communication network architectures: point-to-point and broadcast. [Ref. 2]

In point-to-point architecture, the network normally consists of numerous channels (links). Each channel connects a pair of stations through communications network nodes. The link in the case of sea service is a band of frequency. Often, however, it is impractical for two stations to be directly connected; instead, communication is achieved by transmitting information from source to destination through a network via one or more intermediate nodes. This feature allows for a wide combination of network topologies (point-to-point, multipoint). The purpose of these nodes is to provide a switching facility that will move the information

from node to node until they reach their destination and is not concerned with the content of the information. An important feature when interconnecting nodes which are apart from each other allows for link failure or congestion situations. Figure 1.1 is a generic illustration of the concept. When we have a collection of devices that wish to communicate we will refer to them generally as stations. The stations may be computers, terminals, telephones, or other communicating devices.

In a point-to-point network, if the sequence of links selected for the communication path are used exclusively by the two nodes for the duration of the communication, the technique is called "circuit switching". On each physical link, a channel is dedicated to the connection. Note that the connection path is established before data transmission begins. This channel capacity must be reserved between each pair of nodes in the path, and each node must have available internal switching capacity to handle the requested connection. The most common example of this technique is the public telephone network where all the links between the caller and the recipient of the call will be held until the end of the call. If any one of these links or the node of the network is busy or fails, the call cannot be completed.

Another technique, called "store and forward", exists when the links can be shared by other communications paths, and the information at the intermediate nodes may be stored
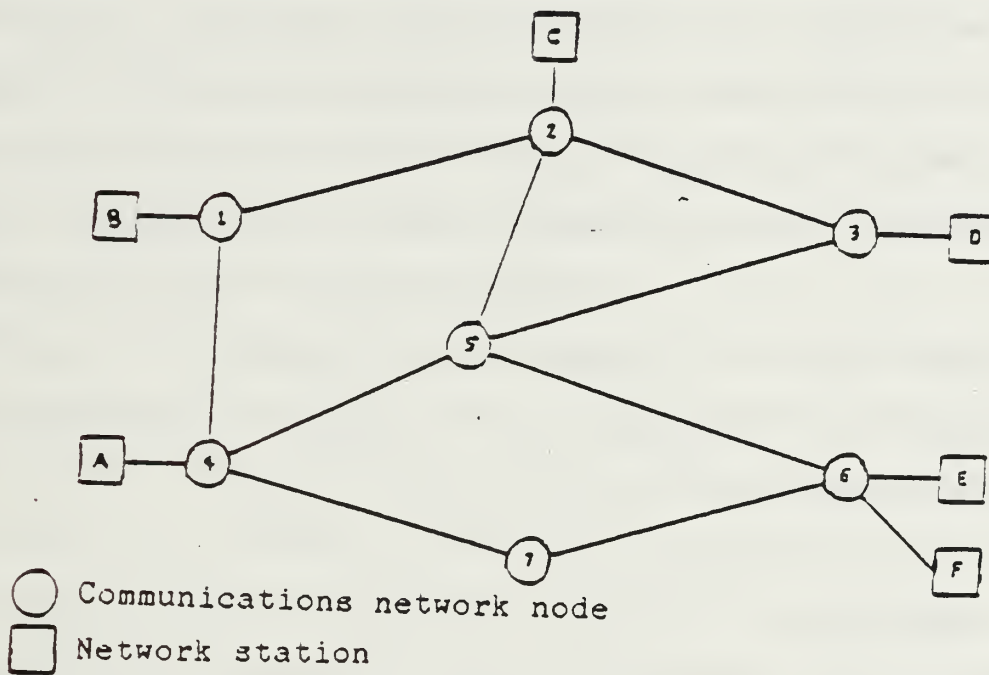
Figure 1.1   Generic Switching Network.

there until the required output link is free to forward. Also, other advantages include the ability to provide simultaneous transfer of information to different stations in the network and the use of high speed links.

With a broadcast communication network, there are no intermediate switching nodes. Each station is attached to a medium shared by other stations. There is a single link shared by all nodes, so that information sent by any node is received by all other nodes. Satellite networks, bus local networks and ring local networks are some examples of this type. Since there is only one path, the total overall transfer rate of information is limited by the path bandwidth and capacity and a single failure may cause complete system failure.

E. OBJECTIVES

The result of the thesis is an architecture which provides three characteristics: [Ref. 1]

* Improved HF performance.
* Packet switched interconnection capabilities.
* Full integration across the radio spectrum.

II. **LINK INTEGRATION**

A. GENERAL

In the previous chapter we discussed the four basic problems that make ship-shore communications different than conventional communications. In this chapter, we examine the ship-shore communications problem in a larger sense than HF. This is done because at the bottom there is a very important principle which makes ship-shore communications different in nature than shoreside communications.

First, we begin an exposition of the concept of a communications protocol, next we provide the basic International Standard Organization (ISO) reference model and define the several layers of standardized protocol structures. A general overview is provided for conventional networks and for ship-shore links and we close this chapter with an introduction to the factors which affect the problem of ship-shore communication.

B. PROTOCOLS

In order to simplify design complexity, most networks are organized as a column of layers or levels, in such a manner that one is built upon its predecessor, and contains protocols. This is the view of the now famous Open Systems Interconnections (OSI) model.

23

Although the OSI model is almost accepted as the basis in this area, there is another point of view which grows out of the extensive research and practical experience of ARPANET. This viewpoint is characterized by a hierarchy of protocols adopted by the International Standards Organization (ISO) to facilitate the interconnection of data-processing devices, as shown in Figure 2.1 [Ref. 3].

The concepts of distributed processing and computer networking imply that entities in different systems need to communicate. In general, an entity is anything capable of sending or receiving information and a system is a physical distinct object that contains one or more entities. For two entities to successfully communicate, they must speak the same language. What is communicated, how it is communicated, and when it is communicated must conform to some mutually acceptable set of conventions among the entities. The set of conventions is referred to as a protocol, which is defined as a set of rules governing the exchange of data between two entities. The key elements of a protocol are [Ref. 4]:

* Syntax, which includes data format, coding and signal levels.

* Semantics, which includes control information for coordination and error handling.

* Timing, which includes speed matching and sequencing.

An example of a protocol is the High-Level Data Link Control (HDLC). The data to be exchanged must be in frames of a specific format (syntax). The control field provides a

24
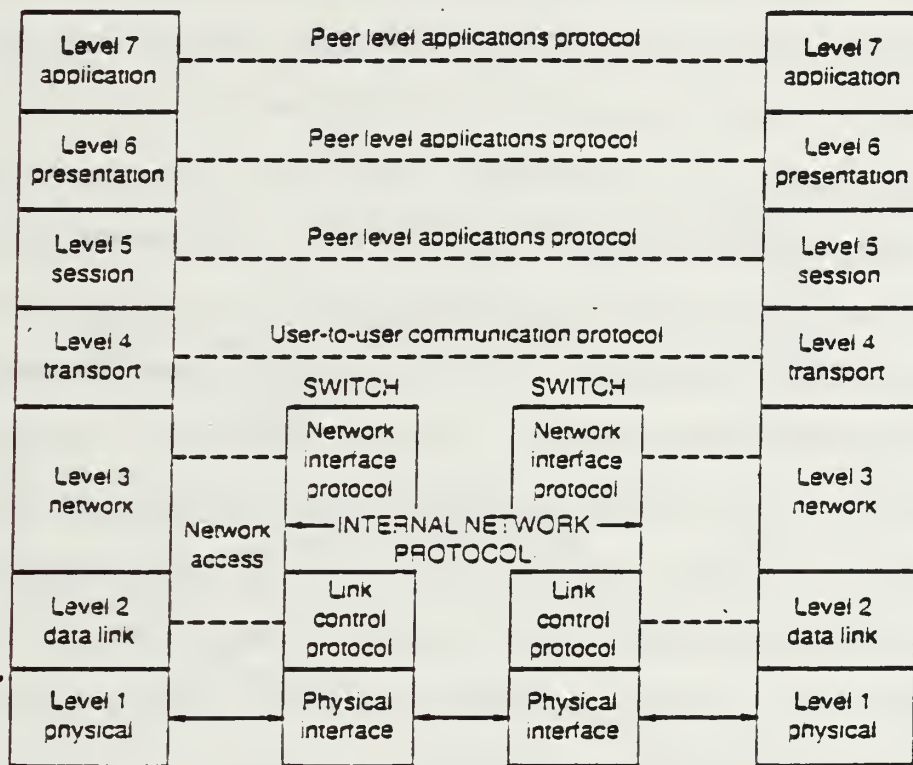
Figure 2.1   International Standards Organization
(ISO) Protocol Hierarchy [Ref. 2].

25

variety of regulatory functions (semantics), and provisions are included for flow control (timing).

Figure 2.2 suggests, in general, a structured set of protocols and shows the most extreme case of two stations connected via multiple switching networks. Between each like pair, an application-oriented protocol is needed to connect the application modules using the same syntax and semantics. The network services entity will have a process-to-process protocol with a coordinating entity to the other station. The first protocol need know little about the intervening communications facility, but makes use of a network services entity, while the second protocol might handle such matters as flow control and error control. Between station 1 and network A, and between station 2 and network B, there must be another protocol. In the case of a broadcast network, this protocol would include medium access control logic. In the case of a packet-switched network, logic for virtual circuit establishment is needed. Internal to each network, a node-to-node protocol is required between each connected pair of nodes, and an entry-to-exit protocol might be used. Finally, an Internetwork protocol is required between the two networks.

Protocol functions can be categorized into the following groups [Ref. 4]:
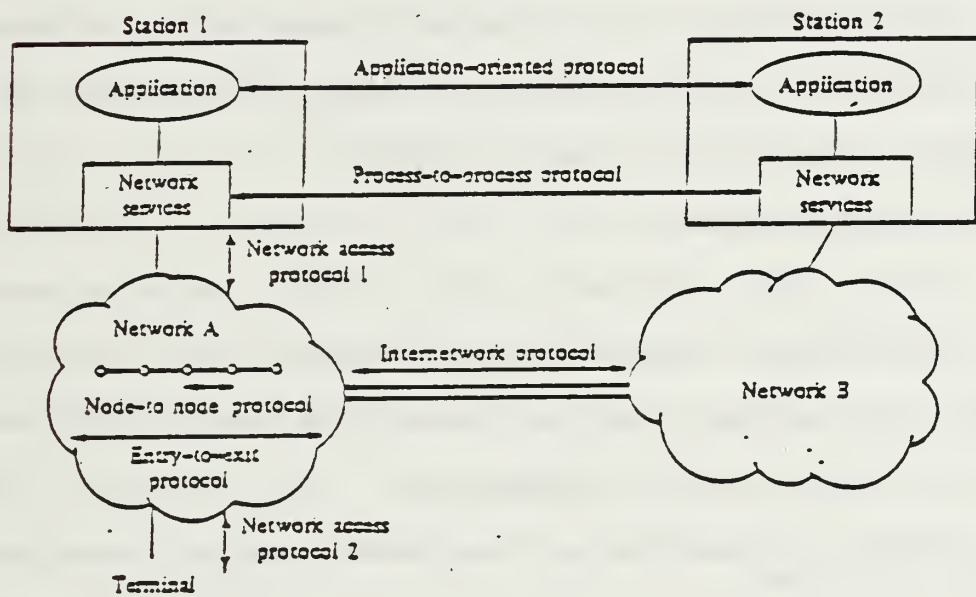
Figure 2.2   Relationship among Communication Protocols.

1. Fragmentation and Reassembly

The main purpose of a protocol is to exchange streams of data between two entities, characterized as consisting of sequence blocks of data of some bounded size. At the application level, we refer to a logical unit of data as a message. Now, whether the application entity sends data in messages or in a continuous stream, lower level protocols may need to break the data up into blocks of some smaller size. This procedure is called fragmentation. A block of data exchanged between two entities via a protocol is referred as a protocol data unit (PDU).

2. Encapsulation

Each protocol data unit (PDU) contains not only data, but control information. Also some PDUs contain only control information and no data. The control information falls into three general categories:

* Address: The address of the sender and/or receiver may be indicated.

* Error detecting code: Some sort of frame check sequence is often included for error detection.

* Protocol Control: Additional information is included to implement the protocol functions.

3. Connection Control

An entity may transmit data to another entity in an unplanned fashion and without prior coordination. This is known as connectionless data transfer. A logical association, or connection, is established between two entities. Three phases occur:

28

* Connection establishment

* Data transfer

* Connection termination

With more sophisticated protocols, there may also be connection interrupt and recovery phases to cope with errors and other sorts of interruptions.

4. Flow Control

Flow control is a function accomplished by a receiving entity to limit the amount or rate of data that is sent by a transmitting entity. The simplest form of flow control is a stop-and-wait procedure, in which each PDU must be acknowledged before the next PDU is sent. More efficient protocols involve some form of credit provided to the transmitter, which is the amount of data that can be sent from the transmitter without an acknowledgement. An example of this procedure is the sliding-window technique. Flow control is a function that must be implemented in several protocols.

5. Error Control

We need techniques to guard against loss or damage of data and control information. Most techniques involve error detection, based on a frame check sequence, and PDU retransmissions. Retransmission is often activated by a timer. If a sending entity fails to receive an acknowledgment to a PDU within a specified period of time, it will retransmit. As with flow control, error control is a

function that must be performed at various levels of protocol. The network access protocol should include error control to assure that data are successfully exchanged between station and network, and the process-to-process protocol should be able to recover this loss.

6. Synchronization

A protocol entity needs to remember a number of parameters, such as window size, connection phase, and timer value. These parameters can be viewed as state variables and they define the state of the entity. It is important that two communicating protocol entities be simultaneously in a well-defined state, for example at initialization, checkpointing, and termination. This is called synchronization.

The difficulty, in this case, is that an entity knows of the state of the other only by virtue of received PDUs. These PDUs do not arrive instantly, they take time to traverse from sender to receiver. Furthermore, they may be lost in transmission.

7. Sequencing

The function of sequencing is to identify the order in which PDUs containing data were sent by numbering them, modulo some maximum sequence number. This function only makes sense in the context of connection-oriented data transfer. Sequencing serves three main purposes:

* Ordered delivery

*   Flow control

*   Error control

    8. **Addressing**

    In order for communication to exist between two entities, other than over a point-to-point link, these two entities must somehow be able to identify each other. On a broadcast network each attached station looks for packets that contain its identifier. On a switched network, the network needs to know the identity of the destination in order to set up a connection for routing data. A destination consistes of names, addresses, and routes. A name specifies what an object is; an address specifies where it is; and route specifies how to go there.

    9. **Multiplexing**

    Multiplexing can be used in one of two directions:

*   **Upward multiplexing,** occurs when multiple higher-level connections are multiplexed on, or shared, with a single lower level connection. This may be needed to make more efficient use of the lower-level service or to provide several higher-level connections in a situation where only a single lower-level connection exists.

*   Downward multiplexing, or splitting occurs when a single higher-level connection is built on top of multiple lower-level connections. This technique may be used to provide reliability, performance, or efficiency.

    10. **Transmission Service**

    A protocol may provide a variety of additional services to the entities that it uses. The three most common are:

31

* Priority: This can be assigned on a message or on a connection basis.

* Grade of service: Certain classes of data may require a maximum delay threshold.

* Security: Security mechanisms, restricting access, may be involved.

C. THE LAYERED APPROACH: THE OSI MODEL

When work is done that involves more than one computer, additional elements are needed. These elements are hardware and software to support the communication between or among the systems. But communications hardware is reasonably standard and it presents a few problems. If communication is desired between heterogenous machines, then the software development effort is a nightmare [Ref. 5]. For these reasons, the International Standard Organization (ISO), established an Open System Interconnection (OSI) model in 1977, which is a framework for defining standards for linking heterogenous computers and as a basis for people to speak the same language in the communications business. OSI provides the basis for connecting "open" systems for distributed applications processing. By the term "open" we mean the ability of two systems conforming to the reference model and the associated standards to connect. The OSI reference model is organized as a series of seven layers or levels, each one built upon its predecessor. The different layers of this model are [Ref.5]:

* Physical layer

* Data link layer

* Network layer

* Transport layer

* Session layer

* Presentation layer

* Application layer

The purpose of each layer is to offer certain services to the higher layer, shielding them from the details of how the services offered are actually implemented.

The lowest level of the ISO reference model is the physical layer. This layer deals with the actual transmission of the raw bit stream over the communication medium. The physical layer covers the physical interface between devices and the rules by which bits are passed from one to another. By physical interface to the network we refer to the pin conections (mechanical characteristics), electrical voltage level and timing of voltage changes (electrical characteristics), signal formats (functional characteristics), and the sequence of events for transmitting data (procedural characteristics). Its main purpose is to ensure that if a "1" was sent, the receiver gets a "1" and not a "0". No consideration is given to the information content of bits or characters or frame boundaries. In the case of ship-shore communications, this layer can further be broken into two subordinate parts:

* The analog waveforms in the HF environment. This inclu-
the ionospheric medium, radio and antenna equipment.

* A baseband layer including modems and link cryptographic devices.

Level 2, known as the data-link layer, moves one step away from the physical layer. Its purpose is to present the network with an error free communication link. The data link layer attempts to make the physical link reliable and provides the means to activite, maintain, and deactivite the link. This involves the division of data into frames, and the corresponding mechanisms to transmit them sequentially, detect any error in their transmission, and process the acknowledgement sent back by the receiver. Since the physical layer merely transmits a stream of bits without concern to their meaning or structure, it is up to the data link layer to create and recognize frame boundaries. For nonswitched networks, or the interface of simple terminals with computers through point-to-point services, generally only levels 1 and 2 are required. Networks designed by a single manufacturer around a single product line, generally do so with a combination of level 1 and level 2 protocols. So, this layer is also broken into two subordinate parts for our ship-shore communications:

* The packet assembly/disassembly portion. Metaphorically, this can be likened to information which is carefully copied into a chunk of data, inserted into an envelope and ensuring that the envelope is sent to the correct destination. At the destination, the envelope is opened and this layer unwraps the data.

* The network access problem. In this case, only one transmitter can be sending at any one time if a packet is to be successfully delivered.

34

A big part of this thesis is an effort to integrate a heterogenous collection of data link and physical layers into a complete network.

The next level, the Network layer, is designed to facilitate communication between systems across a communications network. It determines the main features of the units of information, packets, and how they are exchanged and routed through the network. Also, it defines one of the most protocol-driven functions, the packet interface or the internal network. This layer is also called the Communication Subnet layer, since it receives messages, divides them into packets and ensures that they are correctly received at their destination in the proper order (flow control). This layer also determines the kind of service the network will provide, virtual circuit or datagram (see Appendix A), and thus it contains the corresponding procedures to handle it. For our case of sea service communications we divide this layer into two subordinate parts as well:

* The Network protocol consists of the lower half of the Network layer and is concerned with the network level acknowledgment system.

* The internet protocol consists of the upper half of the network layer and is concerned with interconnections to different networks creating larger communications systems, referred as catenets.

The transport layer, also known as the host-host layer, accepts data from the session layer, splits them into smaller units (segments or packets) if needed, passes these

to the network layer, and assures that the message segmentation takes place and that the message is properly delivered. It creates a distinct network connection for each transport connection required by the session layer, as shown in Figure 2.1, or may multiplex several transport connections on to the same network connection, to reduce the cost. In all cases, the transport layer makes these network connections transparent to the session layer. This layer is a true source to destination or end-to-end layer, so a program on the source node carries on a conversation with a similar program on the destination node, using message headers and protocol messages. In contrast, at lower layers the protocols are carried out by each node and its immediate neighbors.

Level 5, the session control level, represents the true user interface to the network. It establishes the logical connection between user or presentation-layer process in different nodes and maintains and releases it at the users request. To do this it converts names to addresses, checks for access permission, and type of communication (half duplex), etc. It also provides connection services such as recovery, diagnostics and statistics (mainly for performance measurments). In some networks the session and transport layers are merged into a single layer.

The presentation layer performs functions that are requested sufficiently often by the user. It is better to

have the system provide them as services, rather then each user to perform them in its own way. These services include any conversion of information that might be needed as it is transferred between end users. Examples of presentation protocol are data compaction, expansion, encryption, sending and receiving formats, conversion of data types and data representation, terminal handling and fille transfer.

Level 7, application layer, represents the highest level layer in the ISO reference model. It includes applications that are to be run in a distributed environment. Its contents usually depend on the individual users, since they are the ultimate sources and destination of information passing through a network. The application layer does not become directly involved in communication functions, and thus the need for the end user to know about internal is eliminated. It would typically include vendor-provided programs of general utility, such as electronic mail, a transaction server, a file transfer protocol, and a job manipulation protocol. The presentation layer represent the domain of the network users, while the lower level layers represents the domain of the network designers [Ref.2].

D. CONCEPTUALIZING NETWORKS

1. Conventional Networks

The characteristic of conventional communications is that of a full duplex channel at the physical level. This

37

usually requires two separate transmission paths so two stations can simultaneously send to and receive data from each other. Figure 2.3 gives a full duplex view of conventional LANs.

But this feature is not isolated to the physical layer, it affects the link and network layers in the existing standards. The X.25 standard, which is typical in this regard, uses a level acknowledgment system that can be illustrated using a Structured Analysis and Development Technique (SADT), which is a methology for systems engineering and complexity management.

Figure 2.4 presents the structure of a conventional local area network, in which a packet assembler/disassembler exists at each end of the link, and the feedback loop (acknowledgments) is the reverse of the information channel.

2. Sea service Network

In this case, the key characteristic is the one-way channel. Figure 2.5 illustrates the concept of a one way channel where only one station can transmit and the others receive the transmitted information.

This one-way channel is not incompatible with full duplex systems, it simply can be considered as two one-way links, one in each direction. By using this model of a one way channel, we have built a new system that conforms to most of the needs that we have specified.
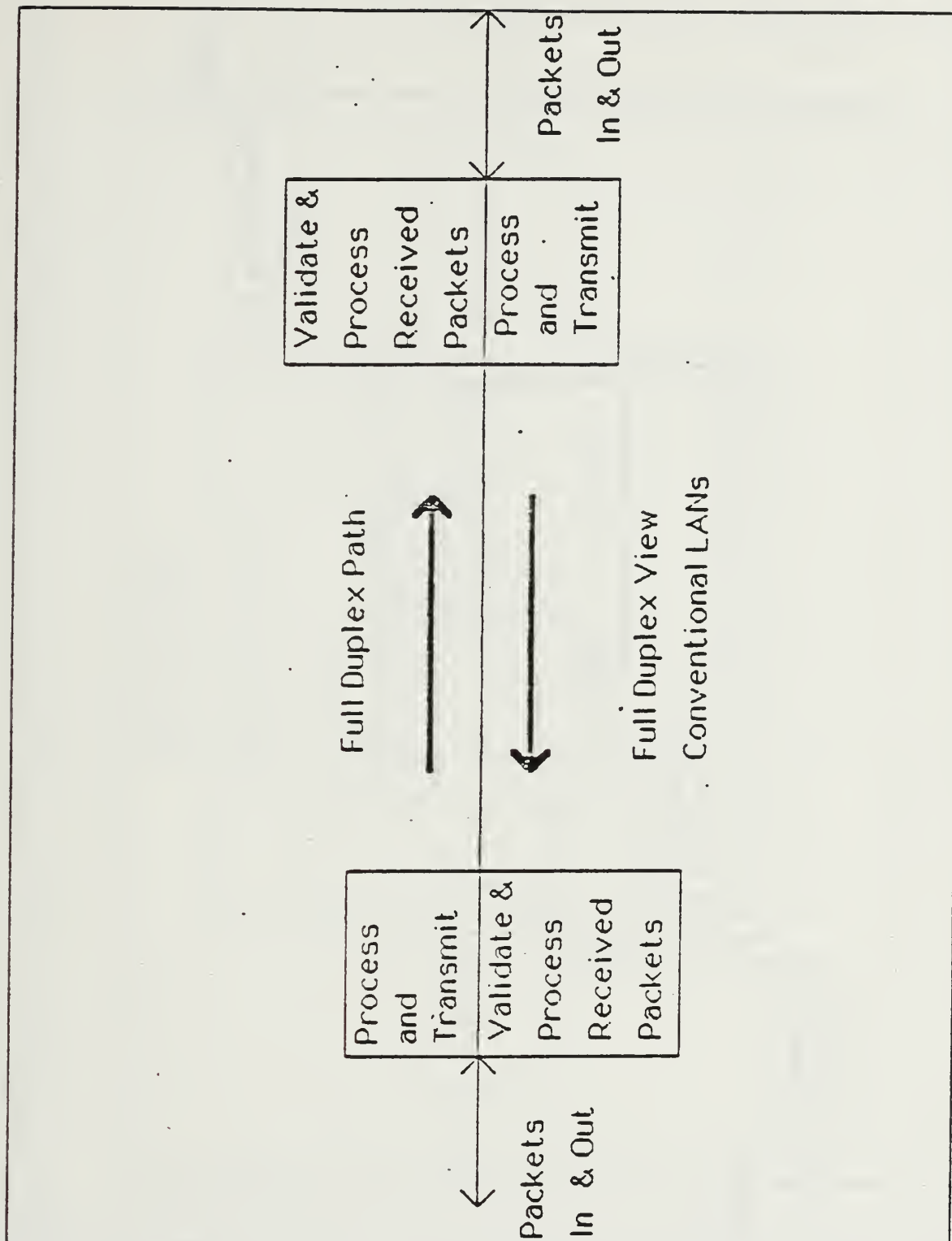
Figure 2.3   Conventional Physical Link Model.
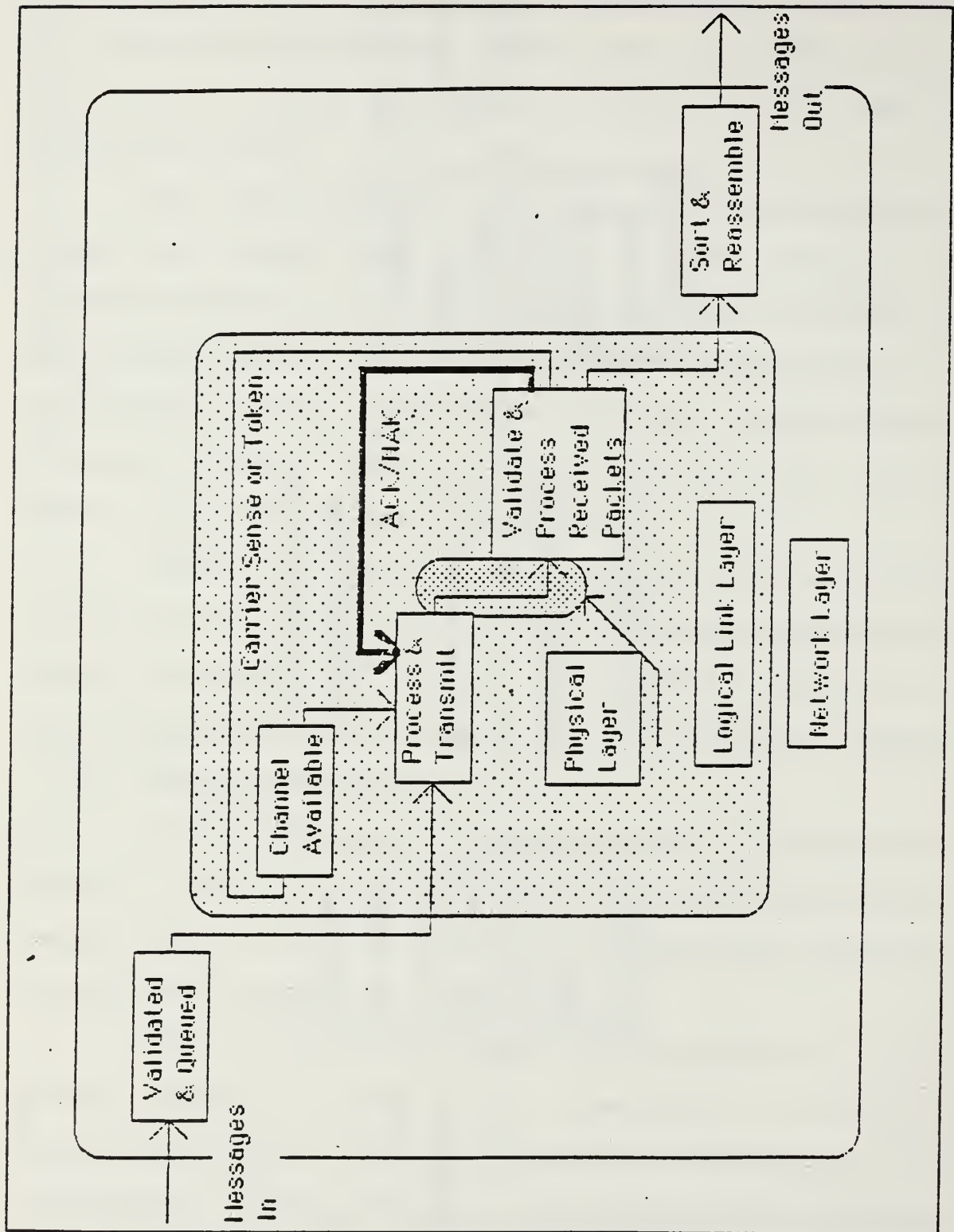
Figure 2.4   Conventional Local Area Network [Ref. 1].
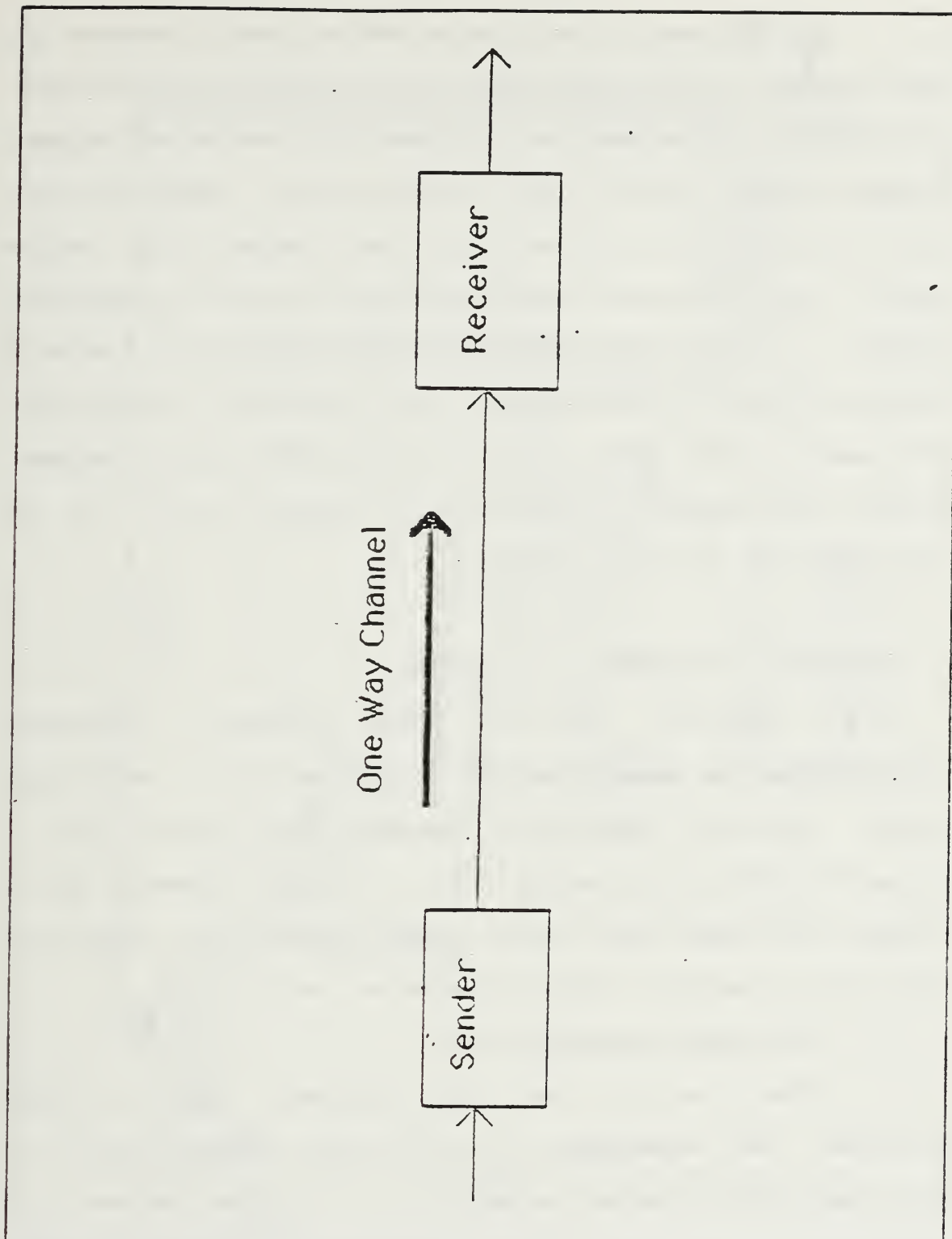
Figure 2.5   Sea Service Conventional Physical Link Model.

41

At the level of protocols and to handle packets, the basic model of a two-way channel must adapt to this problem. Conceptually, this requires a channel for the acknowledgment system from the logical link to the network level, as shown in Figure 2.6. In this way, the feedback loop remains intact, but it has been decoupled from the specific physical channel. It is only required that the receiver have an existing channel to the sender, not a specific return over the same channel that it has received data. Acknowledgment packets are managed like information packets, as far as the link level is concerned [Ref.1].

E. FACTORS THAT AFFECT THE PROBLEM

The primary problem that effects ship-shore communication in general and HF communication in particular is that there is not enough capacity on a single link, no matter how much the capacity of a 3 KHZ channel is, to satisfy the needs of a ship. Other factors that affect the user are grouped into three categories, as follows:

1. Efficiency consideration

Ships can not be full duplex, due to their structure. The wavelength of an HF signal ranges from 10 to 150 meters. This creates significant coupling between the antenna and the ship. With this kind of activity a weak signal cannot be received.
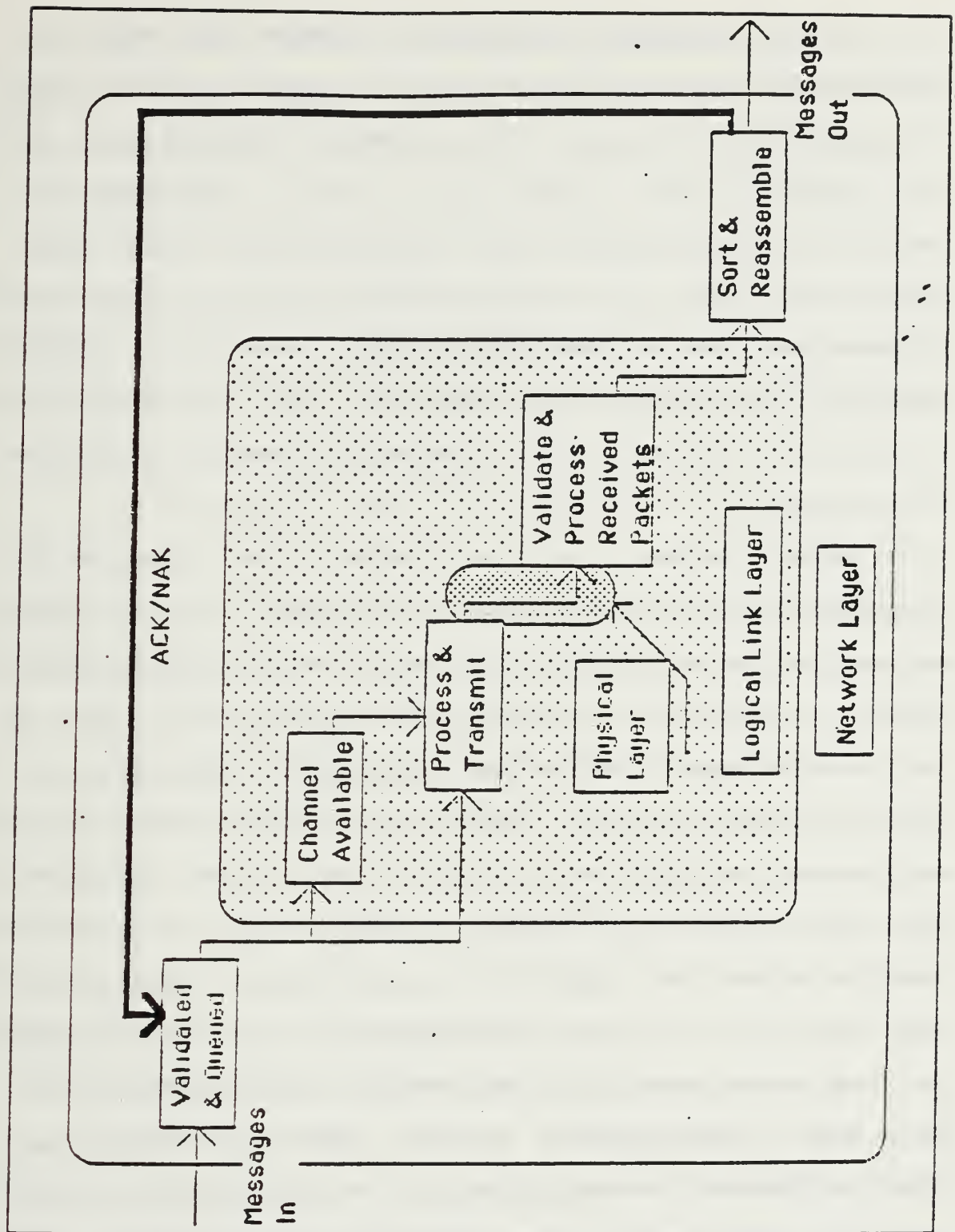
Figure 2.6   Sea Service Network [Ref. 1].

43

Since shipboard antennae are located close together, transmission from a ship may drown out signals that the ship is attempting to receive. This problem is increased and complicated by the "rusty bolt" effect. This effect is created where dissimilar metal joints and corners exist aboard the ship which causes receipt and rebroadcast of transmissions on random frequencies. The "rusty bolt" phenomenon is usually pronounced in the HF band and no filtering on transmitters and receivers solves the drowning-out problem.

Many radios in the ship are packaged as transceivers, where transmitter and receiver are into the same unit. The coupling between these two devices and the antenna is performed by a switch selecting one at a time.

An attempt to solve these problems by emulating full duplex by line reversal is inefficient. Usually, the devices require some preparation time before they start to transmit. High power transmitters require a key-up time. In order to avoid the often poor signal to noise ratios, sea service communications use synchronous communications, which means that they need a synchronizing preamble sent by the modem. Also most cryptographic devices require synchronizing preamble. This synchronizing preamble would be required each time the ship shifts from transmitting to receiving and back.

The only solution to these problems is to use time division multiplexing, where the ship avoids transmission when it is trying to receive.

2. Capacity

As we mentioned above the primary problem is that there is not enough capacity on any single link. The solution to having a traffic load greater than the capacity of a channel is to allocate more channels, assuming for this thesis, fixed bandwidth channels.

In the packet level, if a message is broken up into packets and these packets are sent over each allocated channel, the receiver must reassemble them into the complete message. This solution is known as downward multiplexing and requires network and transport layers.

Another characteristic of sea service communications is the unbalanced traffic. The traffic load of a ship depends on many factors such as tactical, damage, periodical etc. For tactical reasons, a ship may want to receive traffic, but it is not willing to transmit (send acknowledgments) at the same time.

3. Electronic support measure (ESM) considerations.

There are some special characteristics of radio signals in all bands, due to long range transmission and their vulnerability through the atmosphere. These characteristics are more severe in HF due to the large

footprint caused by the worldwide propagation of HF. Some

tactical characteristics are:

* Position localization. The enemy can locate a ship's position when it transmits. This localization is obtained by using cross bearing when intercepting HF signal. This is the reason ships avoid transmission in the HF band when operating under realistic situations.

* Information analysis. Also an enemy who intercepts an HF signal can draw some conclusion about the tactical orders by analyzing who is communicating with whom by analyzing the traffic flow. If we use a decoupling of channels to transmit the traffic flow, it will frustrate this intelligence tactic.

* Interposition. Another vulnerability of the HF signal is that it enables the enemy to interposes into the transmitting frequency when he intercepts and analyzes the signal. This interposition may have bad results, especially in tactical situations when orders must be transmitted.

For these reasons, our system must have the flexibility to allow a ship to transmit in one band (HF band) and

receive in another (satellite band) in an integrated

fashion.

4. Fleet Broadcasts

In the case of the fleet, the Navy has organized

some communications into fleet broadcasts, in virtually

every band that it uses for sea service communications. This

is done for two reasons which depend on the from broadcast's

frequency.

* Bulk. This happens in frequencies below HF, where a transmitter requires a very large antenna and power, factors that are impossible for ships. So, a fleet broadcast for VLF band is used.

* Current Practice. In HF a broadcast is frequently used, although, two way communications is possible as

46

we mentioned. This is done for efficiency and ESM reasons.

5. Communication classes

We can categorize communication into three classes, depending upon the messages [Ref. 1].

* Full ARQ. By this class of communication, full Automatic Repeat Request, we mean how the message is received by the receiver. If the message is correctly received by the receiver, an acknowledgement (ACK) is generated and transmitted to the sender. Incorrectly received message requires a Negative Acknowledgement (NAK) for retransmission by the sender. Primarily ship-shore systems use this method which ensures delivery of a message only when the transmitter receives an acknowledgement.

* NAK only. Negative acknowledgement only assumes that messages are delivered when they are sent. Retransmissions only occur when the sender receivers a NAK. Messages are always numbered in sequence, in order for a receiver to detect a missing message. This method is using the fleet broadcast.

* No ACK. This class of communication is used when it is less efficient to wait for a refresh of the data than it is to request a retransmission.

F. COMPARISON AND CONCLUSION

Conventional networks are modeled as full duplex networks, while ship-shore communication must be modeled as a network with of a single (one-way) physical link. This is the fundamental component that makes sea service communications different from conventional shoreshide communications.

From this chapter we can conclude in two fundamental implications. The first is a decoupling of send and receive channels. A ship can use a different channel then that

receiving the message to close the net. This means that HF, VLF and satellite channels are used complementarily rather then separately in the sea service communications.

The second is the temporal decoupling of an information packet and its corresponding acknowledgment a packet. This means that the system is not required to acknowledge receiving the information packet. A received packet can not be acknowledged immediately, but at a later time which is controlled by the precedence and the content of the packet, and not by the communications system. This is important for submarines, where it is not possible to response immediately to a receiving message.

III. A PROTOCOL FOR NETWORK LEVEL ACKNOWLEDGMENT

A. GENERAL

The purpose of the previous chapter was to show the need for a network layer acknowledgment system for a ship-shore communications network. In this chapter, we are going to set forth a draft protocol to operate under this network acknowledgment system. This network protocol must meld multiple, heterogenous communications links into complete networks, in order to handle any specific link, be it VLF, LF, HF, satellite and/or shoreside telephone.

An interface between network and logical network layer links is described to understand clearly how each layer communicates with superior and subordinate layers. Also a firm will be established between the network layer (node) and logical link layer (link).

This chapter will close with an introduction of the State Information in a network protocol with an example of timeout period (T1) and counter working together.

B. NETWORK PROTOCOL

Since there are not enough data to help us to determine the structure of the network protocol, we will examine how this protocol works with Local Area Networks (LANs) and then

apply the principles of ship-shore communications networks to each component.

There are two key points which help us examine network protocols. These points are the Internet Protocol and Local Area Network (LAN) protocols.

1. Internet Protocol

Two protocols make up the Network layer protocol, as shown in Figure 3.1.

* Internet Protocol (IP).

* Network Protocol (NP).

The Internet Protocol (IP) is used to provide a network layer protocol for the operation of multiple networks and is found in the upper half of the network layer of the ISO reference model.

The Network Protocol (NP) is directly concerned with intra-network communications. Most functions, which are performed by Internet Protocol will not be duplicated by the network protocol, but the two protocols do mesh cleanly.

2. Local Area Network Protocols.

The best known of the network protocols is X.25. The X.25 standard of the Consultative Committee for International Telephone and Telegraph (CCITT) has a strong influence on the development of packet networks around the world and on the design of user equipment to operate with those networks. Therefore, we will adapt what can be collected from X.25 into the Network Protocol.

50
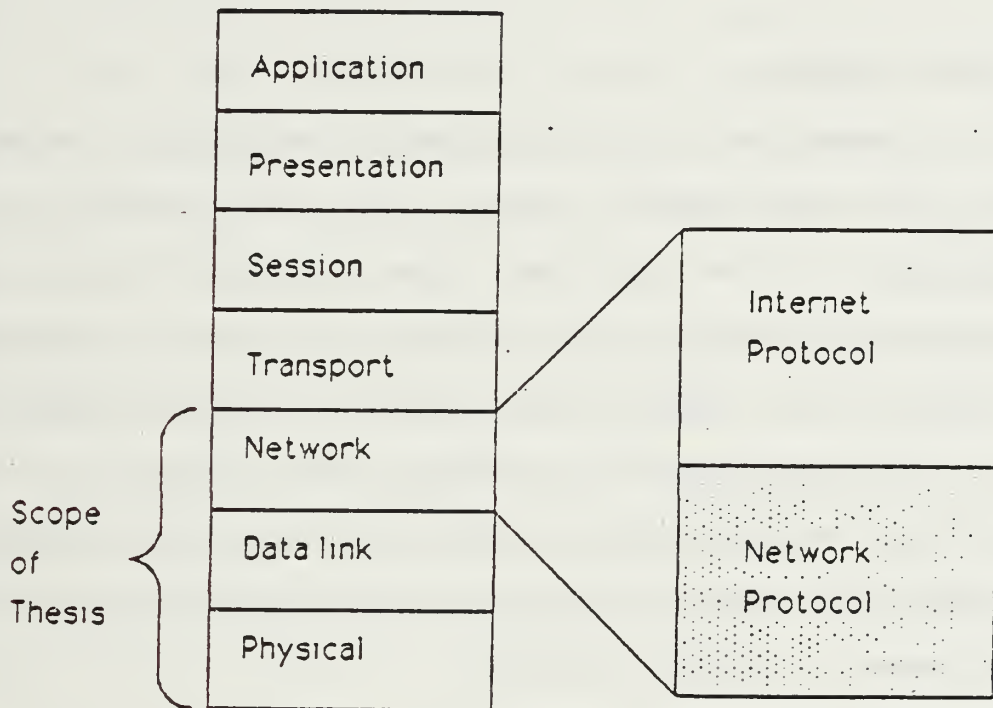
Figure 3.1   ISO Reference Model and Network Layer Division.

Unfortunately, X.25 protocol which is a representative of all Network protocols uses the full duplex physical layer model, which is in contrast to our one way model.

The existing standards of X.25 protocol are not discussed in this chapter. The interested reader is referred to Appendix B.

C. DESIGN ISSUES

The network protocol structure is based upon the packet header of each packet. Some required information is transmitted to the receiver with each packet while other information is supplied by the receiver during processing. For example, the channel identification, the frequency used to provide communication between two stations, is not required to be transmitted with each packet header since it is known to the receiver. Now, we can examine some of the design issues in greater detail.

1. Addressing

Recall from chapter two that a distinction is generally made among names, addresses and routes. A name specifies what an object is; an address specifies where it is, and a route indicates how to get there.

The naming and addressing of entities has no unique solution. In this subsection we are going to outline some approaches and considerations, which are useful for our

research into ship-shore communication networks. The following topics are considered [Ref. 4]:

The **name structure** used for global names, names by which entities are known outside their own systems, can be either hierarchical or flat. A hierarchical name would have the structure SYSTEM.ENTITY, or in the case of multiple networks, NETWORK.SYSTEM.ENTITY. A flat name structure is one in which each entity has a global name that is unique throughout the domain of communication. A hierarchical name has more the flavor of an address than does a flat name, because it is easier to add new names to the universe of names with hierarchical scheme since entity names need only be unique in a system. For the case of flat names, one must check that any new name added to the system is not the same as any previous name. Secondly, a hierarchical name is an aid to routing since it identifies the system containing the entity.

An entity can only send data to or request a connection with an entity whose name it knows. This requires a **name knowledge**, regardless of name structure.

While, for connectionless data transfer, a global name is used with each data transmission, for connection-oriented transfer, it is desirable to use only a **connection name** during the data transfer phase.

A **port name** is a global entity name. If each entity has a single port name, there is not much point to

53

the concept. However, it is often the case that multiple port names are associated with an entity. This can be used to provide multiplexing, as with connection names.

Finally, the **group name** is a name that refers to more than one entity or port and has been used to mean a number of things. One usage is that a group name identifies multiple simultaneous recipients of data. Another usage is to identify a connection group.

One existing protocol for Local Area Network (LAN), X.25, uses a logical address for each subscriber. The flaw in this protocol is that a message addressed to multiple subscribers must be transmitted to each one individually. In sea service operations many units operate together as a group. So, a message is addressed to many destinations, using an addressing scheme that allows multiple addressing to greatly improve efficiency in a constricted bandwidth environment. In the Navy we use a system of call signs, Address Indicator Groups and a Collective Address Designator. This system has the advantage of allowing a communications station to send a packet just once, then count all the acknowledgements of the destination stations. Of course, retransmissions may be required to overcome unreliability and noise, but for this situation the retransmissions will be less than if each destination were serviced individually.

2. Fragmentation and Reassembly

These two functions are required for message identification. Individual channels within a catenet will generally be diverse, and in particular specify different maximum (sometimes minimum) packet sizes. It would be inefficient and unwieldy to try to dictate uniform packet size across networks.

Several points of message identification are required. The following fields in the header are important.

a. ID

The ID is some means of uniquely identifying the channel over which a packet was sent. This ID is necessary to identify the quality of the channel, which depends on the packet arrival condition. If the arrival packets of a specific channel are not in good condition, then a channel adjustment is required and the specific channel used must be known.

b. Length

The length is the space of the data field, which includes the entire message. The message identification is analogous to the Navy's Date_Time group. Since there is some capability for identification inherent in the protocol, it is only necessary to copy the data from the Internet Protocol header to the Network Protocol header.

c.   Packet Identification

To get the complete message at the destination, some information is needed for gluing packets back together. This function is also part of the Internet Protocol and it is not necessary to duplicate it for the Network Protocol.

d.   Packet Offset

The offset is the position of a fragment in the original location. If packets are fragmented into smaller pieces in the course of their travel to meet the requirements of the channel, some control information is needed to reverse the fragmentation and recreate the original message. This is particularly important as the network grows to encompass several diverse types of channels using different packet sizes. The Internet Protocol is not adequate to handle the packet identification by itself.

During the phase of assembling different size packets into a complete message, the assembler can work efficiently if it knows how far each packet starts from the beginning of the message. This overlaying can be effective when packets derived from one channel can overlap those derived from another channel.

Packets received from different noisy channels can be assembled to create a complete message when packet offset and length (Message Identification) can be used to patch them together, as shown on Figure 3.2. For this case an acknowledgment of the complete message instead packets,

56
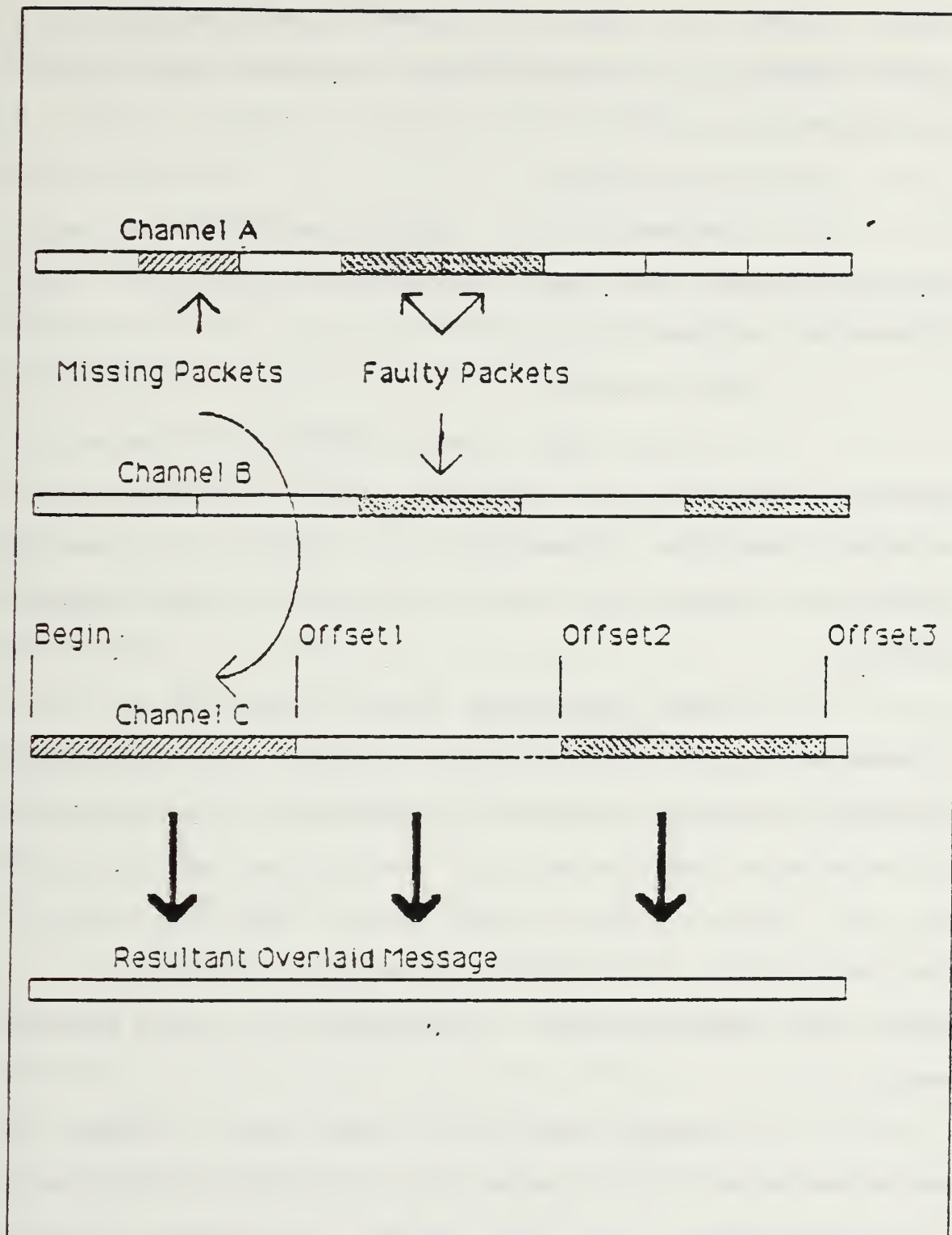
Figure 3.2   Packet Offset Concept.

should cause the sender to cease retransmissions of any packet (parts of the message) which may have been received in some error condition.

3. Control Information

This information is required to control or handle particular packets that were received by the receiver. This information includes [Ref. 1]:

a. Acknowledgments

(1) Full ARQ. Every received packet generates from the receiver either an ACK or NAK, depending on the received packet's situation. The transmitter ensures delivery of message only when it receives an Acknowledgment (ACK/NAK).

(2) NAK only. This type is used for the fleet broadcasts, since the receivers are passive equipments and only service missing packets. This assumes that messages are delivered when they are sent and retransmissions only occur when the sender receives a NAK packet. This also requires some care in the structure of message identification to enable the transport layer to recognize a missing message event.

(3) No Ack. This is a state where a packet is not acknowledged by a receiver. This procedure is used when it is more effective to wait for the next refresh of the data than to attempt to retrieve a damaged one.

The Internet Protocol does not include these issues. It assumes that all packets are to be acknowledged. For these reasons we must include these issues in our Network Protocol.

b. Precedence-Grade of Service Indicator

This information is adequately provided in the Internet Protocol and only needs to be copied to the header of our Network Protocol.

c. Error Freedom

This includes the degree of error in the data which can be tolerated without losing their usabilities. There are data that must be fully error free and data that can tolerate more errors.

This procedure is inadequately considered in the Internet Protocol, since it gives only two alternatives: normal and high reliability without any gradations between them.

d. Lifetime

There are some data which must be discarded if they are not delivered within a certain time frame. This elimination from the communications system is required to ease congestion and allow more current information through. This includes messages of the case of No_Ack and messages where the information expires after a certain time frame, like enemy reports.

In the first case of No_Ack data, outdated packets should simply be thrown away. In the second case of enemy reports, data have chronological significance which indicates that delivery is useful, but not at the original precedence. In this case, the precedence should be downgraded until the point where the message is removed from the existing queue.

The Internet Protocol contains a lifetime parameter, but it is used for a different purpose. This purpose is to eliminate datagrams (messages) that might otherwise loop indefinitely through the net for ever. To avoid these problems, each datagram can be marked with a lifetime. Once the lifetime expires, the datagram is discarded.

A simple way to implement lifetime is to use a hop count. Each time that a datagram passes through a link, the count is incremented. Alternatively, the lifetime could be a true measure of time. This requires that the links must somehow know how long it has been since the datagram or fragment last crossed a link in order to know by how much to increment the lifetime field. This would seem to require some global clocking mechanism. The advantage of using a true time measure is that it can be used in the reassembly algorithm. When a datagram is been reassembled from fragments, the buffer will be cleared of a partially reconstructed datagram if its lifetime expires.

Since our purpose is congestion control and maintainance of a high grade of service during the presence of high loads, the Internet Protocol approach must be modified to meet these requirements. Some packets should be given a lifetime measured in seconds. These can be handled adequately within the Internet Protocol, but this function should be handled as low in the ISO layering as practical. The Network Protocol is the first practical layer to handle the problem.

e. Header Checksum

A checksum in the headers allows a receiver to check for errors in the header that might result when packets are routed to the wrong destinations.

f. Version Number

A version number included in the packet header is used to tell the receiver if this packet is generated from different model senders. Also it allows for incremental updating and avoids the awkward and difficult condition when it is necessary to update all the units listening simultaneously in the same communication area.

4. Flow Control

Flow control is a technique for ensuring that a sender does not overwhelm a receiver with data. In this subsection we are not going to describe the flow control techniques, but how flow control is applied to the case of ship-shore communications. In the beginning, we must

61

consider the data stream. Each link (logical link layer) will demand data at different and varying rates. For example, in the case of the HF environment, packet size, compression efficiency, error code rate and modem baud rate affect the input data rate to a sender, while the requirement for retransmitting packets affects the input data rate. For VLF broadcast a different rate than HF is demanded.

The physical and link level equipment function better with continuous rather than bursty data, so the sender must be able to supply the data stream with a bit rate as fast as they can be transmitted. On the other hand, the receiver demands data from the network at different and varying rates. Therefore, the node (network layer) equipment must have sufficient buffer space to offer and accept data with the speed required by the link termination equipment.

In the case of ship-shore communications, the required data rates for each link are modest compared with those required for Local Area Networks (LANs). Flow control is required for shore side links, but ship-shore links can adjust the systems' size to accommodate our requirements and flow control is not needed.

The data stream itself can be managed as a queue. The node (Network layer) equipment must manage a queue for each sender. Network level acknowledgment considers the ACK/NAK packets with the same precedence as information

packets. For example, a precedence packet must generate a precedence ACk/NAK packet. These ACK/NAK packets should be queued ahead of information packets of each particular precedence. A data stream with each queue management precedence is shown on Figure 3.3.

Also, the node can only queue up a data stream which consists of several packets or several messages preceded by the header of each message. When a sender transmits a packet, it reads the required number of bits from the queue and places the header at the head of the queue. This allows the link and node to operate independently. When the node needs to queue data of higher priority data, the existing into the queue content pushes down the queue and the higher priority data are queued at the head of the queue.

A break must be placed between messages in the queue. When the sender is reading in bits of the data to be sent and meets a break, it stops the packet at the break point.

Before departing from the network protocol and launching into the interfaces chapter we must establish a node-to-link connection for controlling the information port, as we did for the data stream in the flow control subsection.

This port of control information requires that control packets must go to the link control unit through a different channel that the data stream uses. This control
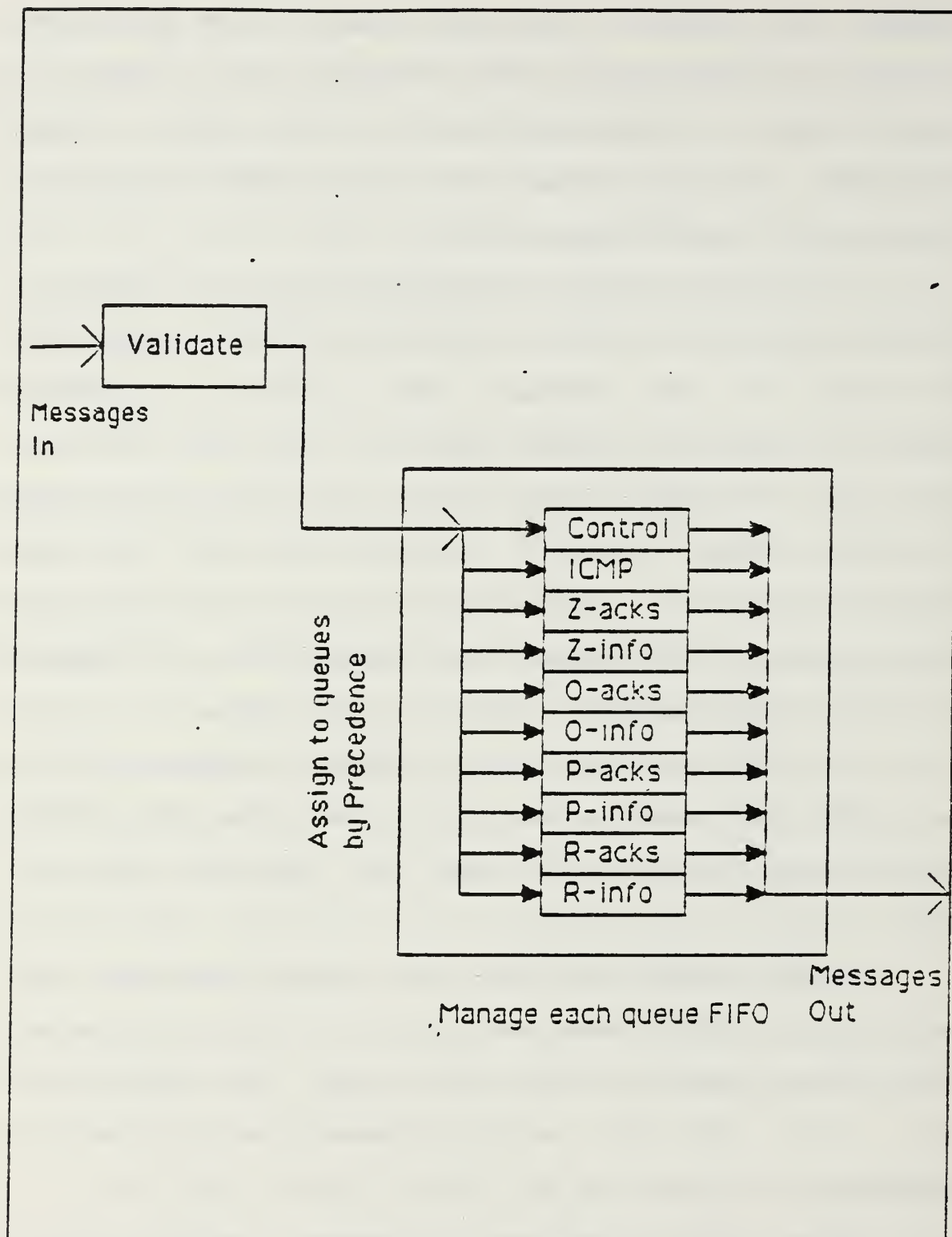
Figure 3.3   Queue Management Concept.

64

information includes the Sequence Order List (SOL), error code rate or bit rate, and control packets generated by a receiver requesting a change in packet size. An additional packet included in this control information is one from a station logging into or out of the link which requires the control unit to allot or delete space in the Sequence Order List.

In the case when more than one HF transmitter are ganged together, a kind of control information is required for the two senders to coordinate transmissions. This information includes a controller which inhibits a senders transmission while the receiver is receiving traffic. This information is only needed for the link to synchronize their transmissions. For our case, this control information is of no value to the node, since we need a set of multiplexing control units for adjacent links connected together.

D. INTERFACES

As with any protocol, network protocol can best be described in three parts indicating how this protocol communicates with superior and subordinate layers. An interface between the network and logical link layers is mandatory to successfully analyze the software problem and to maintain an open architecture.

1.   Network to Internetwork Interface

This the simplest of the existing interfaces. The IP is designed to operate in a catenet consisting of diverse individual networks. Therefore, only a minimum level of service is expected and the requirement is only for an unreliable datagram service. In this case, the Network Protocol passes packets to the Internet Protocol, just as existing network layers do (e.g X.25). Therefore, the Network layer, upper half, and all higher layers will not require any modifications.

2.   Network to Logical Link Layer Interface

This interface is more complex than the previous one. In the network layer we have two types of packets.

a.   Data Packets

Data packets are delivered to the Internet Protocol, just as existing network layers do (e.g X.25), and as mentioned above.

b.   Control Packets

These packets, including all AcKs, are used by the Network Protocol and lower layers and are not delivered to the Internet Protocol or higher layer. These are the materials that make the network level acknowledgement function [Ref. 1].

As we mentioned above, acknowledgment packets have the same precedence as the data packets that created them in the receiver. The receiver must be able to

66

distinguish between them, and treat on ACK packet with the same precedence as the content of the corresponding messages, not on the exigencies of the communications system. This is required to exclude the occasion where a data packet keeps timing out and being retransmitted, thus preempting the ACK necessary to turn off the retransmissions.

Other control packets are necessary for network control purposes, and will not be passed across the boundary of the Network Protocol. Since most of these packets are necessary for maintaining communications, they will have the highest precedence in the communications systems.

3. Multiple ports

The main function of the Network Protocol is to join together several logical links which represent several types of physical media. This requires multiple ports to the Network Protocol with two components at each port.

a. Packet port

This is the port where only data packets are sent or received. The port's service will be in a queue form where the highest precedence packets are inserted at the head of the queue.

b. Control Port

This is the port where only control packets are sent and received and is also a bidirectional port. In this port the control packets cannot wait in the queue; they must

67

be delivered to the sender or receiver just when the network layer receives them.

The result of this Network Protocol is that several functions are performed by it that were formerly done by the logical link layer. This simplifies logical link design, which is beneficial because there are several efficiency problems that must be dealt with there, and are not as severe in conventional networks as in the ship-shore system. [Ref. 1]

E. STATE INFORMATION IN A NETWORK PROTOCOL

In previous sections we described the information needed in the packet header. As we noted, the packet header contains the destination address to which the packets are to be delivered together with control information needed to control the movement of the packets through the network.

With the exception of the packet header information, there exist an additional information which is not sent by the packets. This kind of information is stored with the transmitted packets in a pending area that is called waiting queue. This information includes:

1. <u>Timeout Period</u>

This is the amount of time that elapses before an unacknowledged packet is resent. These acknowledgement packets are the key to the error detection mechanism that insures integrity and accuracy of the transmitted data.

68

Any information packet that is properly received is immediately acknowledged back to the sender with one acknowledgement packet. In this way the sending switch knows that the information packet has been received properly by the destination. Then the packet is removed from the waiting queue and logged on archive as sent and acknowledged.

If an acknowledgement is not received within a certain time domain, known as T1 in X.25, the packet comes back to the send queue and is resent. The retransmission of the packet is not required to be through the same channel as the original packet was sent. Then the packet returns to the waiting queue, but now with a new timeout period (T1). All the above procedure of packet state transmissions is illustrated in Figure 3.4.

2. Integral Counter

To avoid an infinite number of retransmissions, in the case where the timeout period (T1) expires without acknowledgment, an integral counter is required. Each retransmission causes the integral counter to be incremented. At some predetermined point of retransmissions, the system gives up, changes the value of the timeout period (T1) or informs the operator that the communication with the destination has been lost.

3. T1-Counter in Common Structure

The timeout period (T1) and integral counter can be implemented properly together in the same structure. Let's
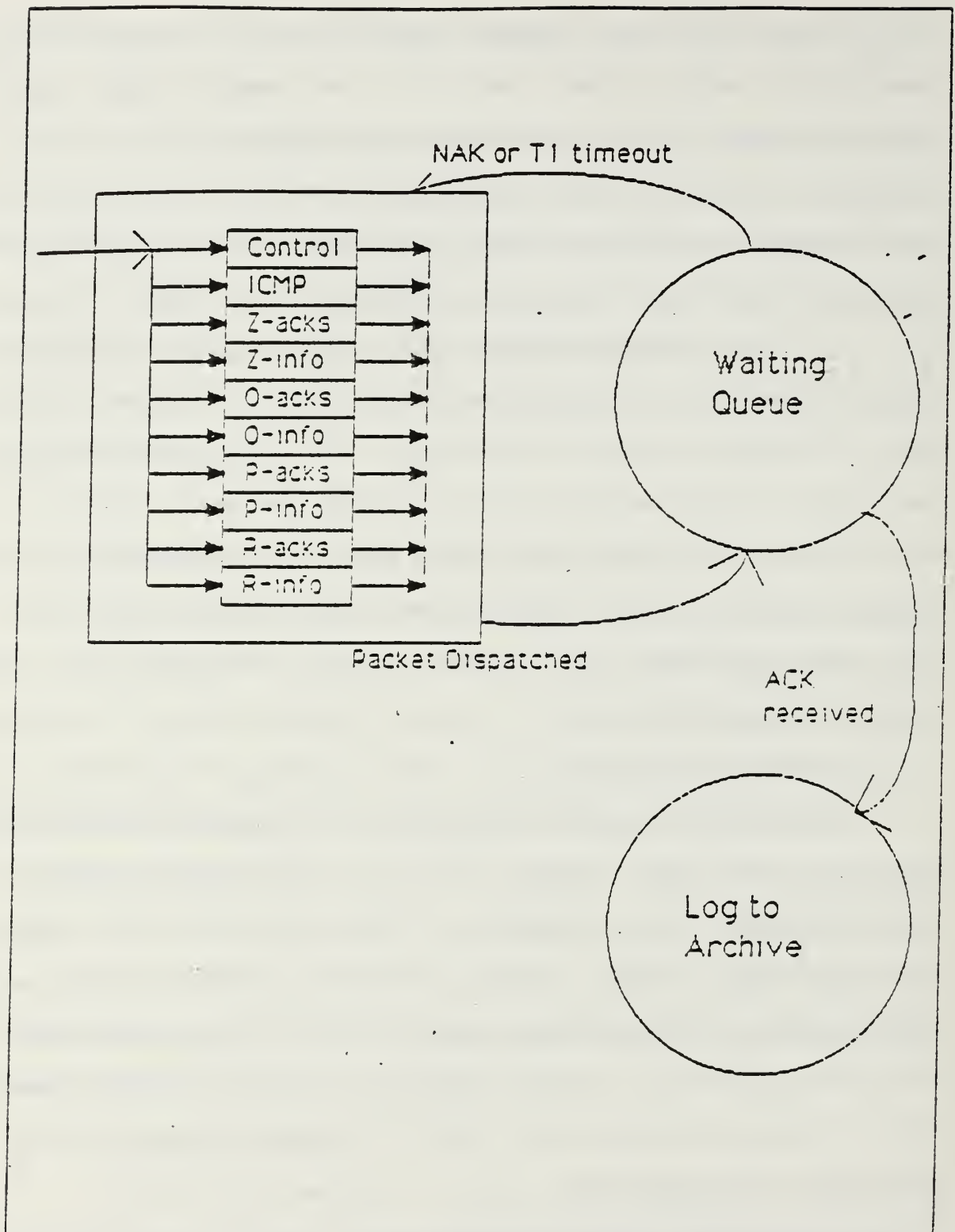
Figure 3.4   Packet State Transmissions.

70

examine this structure by reference to a particular example. Let's assume that we want to sent a high precedence message. Due to the high precedence, the required grade of service is quite high and the timeout period is set quite short. We have the following cases:

When a transmitter sends a packet to the receiver, the packet leaves the sender queue and goes to the waiting queue. The receiver from the other side, receives the packet correctly and responds with an ACK packet. When the sender receives the ACK packet, it informs the waiting queue and the packet is logged on archive as sent and received.

The receiver is unable to acknowledge in the defined timeout period (T1) for any reason, such as congestion, EMCOM, error packet. So, timeout period (T1) expires and the packet is restored to the sending queue for retransmission. After a predetermined number of retransmissions, four for example, the counter causes the timeout period (T1) to be reset to a longer time domain. If at any time during this process, an acknowledge is received by the sender, the above process is stopped and the packet is logged into the archive as sent and received.

In the case where the receiver gets an incorrect packet before T1 times out, the receiver is able to return a NAK packet to the sender. This process immediately causes the sending packet to be removed from the waiting queue for retransmission.

71

The above algorithm is complete for ARQ packets. For NAK-only and No-ACK packets only parts of the algorithm must be skipped to complete the process for these particular packets. The NAK_only procedure requires that all packets be considered delivered, unless otherwise noted. This causes the sending packets to be logged as they are transmitted. With this procedure the NAK packets must be available to be retrieved and transmitted.

A general technique, known as majority voting will be explained in the details of chapter 5. If the counter completes its predetermined number of retransmissions, for example four times, without receiving an ACK packet and before resetting T1, then the receiver will have the packet four times to vote on faulty packets. If a correct packet is received during this procedure, then an Ack packet is originated which causes the process to stop and logs the packet into the archive.

All the above algorithms were described for one sending packet only. This T1-counter structure can be used for many packets by multiplying the process for each packet. It can also be used for the case of collective addressing by maintaining a T1-counter structure for each address. The procedure is that a sender transmits packets, marked for a collective address, the packet is removed from the sending queue to the waiting queue. Then it waits there, until an acknowledgement is received from each address. Until all

72

acknowledgements have been collected, the packet remains in the waiting queue subject to timeouts and NAKs before it is logged on archive.

IV. NETWORK ACCESS -- UPWARD MULTIPLEXING

A. GENERAL

The purpose of the previous chapter was to set forth a draft protocol to accomplish the network layer acknowledgment. In this chapter the discussion moves down one layer in the OSI reference model to examine data link protocols.

Since the main function of the data link layer is to pass data and control information to the next node, the objectives of transmission protocol will be described first. Then, the problems are described, which make use of of conventional network access methods inefficient, with a review of each access method. Also in this section are described the requirements to use synchronous equipment, although asynchronous transmission is better.

An algorithm for network access control in an multiplexed environment will be described for each of the following systems:

* Full duplex system
* Simplex polled circle system
* Half duplex system

The chapter will close with a comparison between the above three systems with a determination of the best option as applied to sea service communications.

74

B. A FIRST APPROACH

  1. Objectives of Transmission Protocols

    In order to move data from one point to another,
sender and receiver must agree on a transmission protocol.
Protocols have the following objectives. [Ref. 6]

    a. Delineation of Data

      Transmission of data includes not only data
messages, but also control information and almost always
information for error detection. Receiving stations must
always be able to distinguish which is which, meaning that
the protocol must enable receivers to determine where the
data portion of the messages begins and ends, where the
control portions of the message are, what they mean, and
where the error control bits or characters are. Delineation
of data is illustrated in Figure 4.1(a).

    b. Error Detection

      This function is performed by data link
protocols to generate, append, and forward error detection
codes. Protocols differ with respect to the specifics of
their error detection algorithms and with respect to where
in the message the error codes are placed. The error
detection function is depicted in Figure 4.1(b).

    c. Addressing Capability

      Most data link protocols use a type of
multistation configuration. For multiple stations to share a
circuit, the data link protocol must enable a device

75
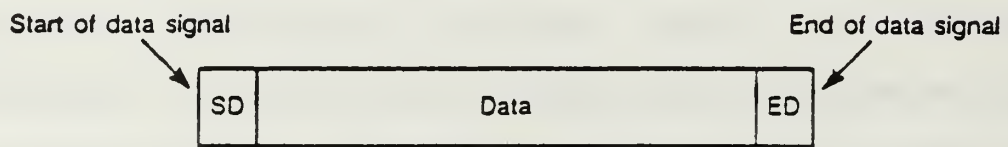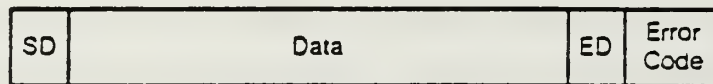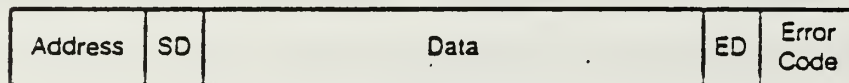
Figure 4.1   Some Data Link Functions.

address to be appended to the message. Each addressable device in turn must know where the address is in the message, usually at or near the beginning. Addressing is illustrated in Figure 4.1(c).

d. Connection Control

Data link protocols must be able to set up the occasions under which a station can transmit and receive data. In the case where two or more stations can transmit at once and so interfere with one another, then the protocol must recover from such a situation.

e. Transparency

This function refers to the ability to transmit any bit pattern as data and have it accepted correctly. This sounds usual, but it is not in reality. It is true that transparency is hardly ever an issue in transmitting data to terminals, since all transmitted characters are displayable characters in the code set, that is, characters that represent letters, numbers and special characters. There are many code sets, such as American Standard Code for International Interchange (ASCII) and Extended Binary Coded Decimal Interchange Code (EBCDIC), which reveal that certain bit sequences, such as End Of Transmission (EOT) are assigned control functions and are not displayable characters. The ASCII is implemented primarily as a 7-bit code, although an extended 8-bit version also exists. The EBCDIC is implemented as an 8-bit code to form a character.

77

In the case where such special control bit sequence are to be transmitted as data, the data link protocol must not interpret them as control characters.

f. Code Independence

This is the ability to successfully transmit data with any coding scheme, such as ASCII, EBCDIC, etc. This function enables two different devices, for example one that uses ASCII and one that uses EBCDIC, to share a line. Some of the protocols provide no code independence, although higher-level data link protocols usually do. Code independence is not a requirement, but a desirable characteristic, as with addressing.

g. Multiple Configurations

This objective is not applicable to sea service communications. In a conventional network this enables the system designer to plan a network topology that is consistent with the application and that takes full advantage of the capabilities of the devices being used.

h. System Growth

Data link protocols should be capable of supporting new hardware components and features added to old hardware.

i. Efficiency

A protocol with very little overhead is desirable due to the restricted bandwidth in an HF environment. Overhead refers to the additional number of

78

characters or bits that must be appended to the messages in order to meet the previously defined objectives, thus allowing more channel capacity to be devoted to carrying data. Although data link control is frequently considered as overhead, it really is a necessary function, not just overhead.

   2. Upward Multiplexing

   Upward multiplexing means that multiple high level connections are multiplexed on, or share, a single low level connection. This may be needed to make more efficient use of the low level service or to provide several high level connections in an environment where only a single low level connection exist. This is applied to sea service communications when several ships share a single frequency with the communications station. In this case, the problems which arise are: How they share a communication channel, who uses a communication channel in a network and when channel access occurs.

   When a network is used, only one station should transmit at any moment. If any station violates this rule, then collisions occur and transmission is impossible. A protocol is required to protect the network from collisions and provide successful channel access. Network access protocols are designed to deal with this problem and prescribe rules to either prevent or deal with the network collisions.

3. Data Link Layer Division

As was mentioned in chapter 2, the OSI model describes the functions of a communication subsystem within the three lower layers. The operations described in the present chapter are functionally located within the data link (second) layer of such an architecture. The link layer is split into two sublayers. [Ref. 7]

* Network Access protocol, which performs the logical control of the particular medium access protocol.

* Packet structure and handling, which performs the addressing and link association handling functions.

This division of data link layer into subcategories is illustrated in Figure 4.2.

In this chapter, we confine ourselves to the the problems of the first of the above protocols, especially in HF communications environment. In this environment, we are confronted with the one-way nature of the bands above and below HF frequency. For bands above HF, specifically satellite channels, there exists the problem where stations cannot hear each other. Satellite communications can operate on some assumptions that do not hold true in the HF band, so we are dealing with the more difficult of the two problems [Ref. 1]. Anyway, one solution for sea service communications is borrowed from the satellite system. For bands below HF, network access is not a problem, the only transmitter on the network is the communications station.

80
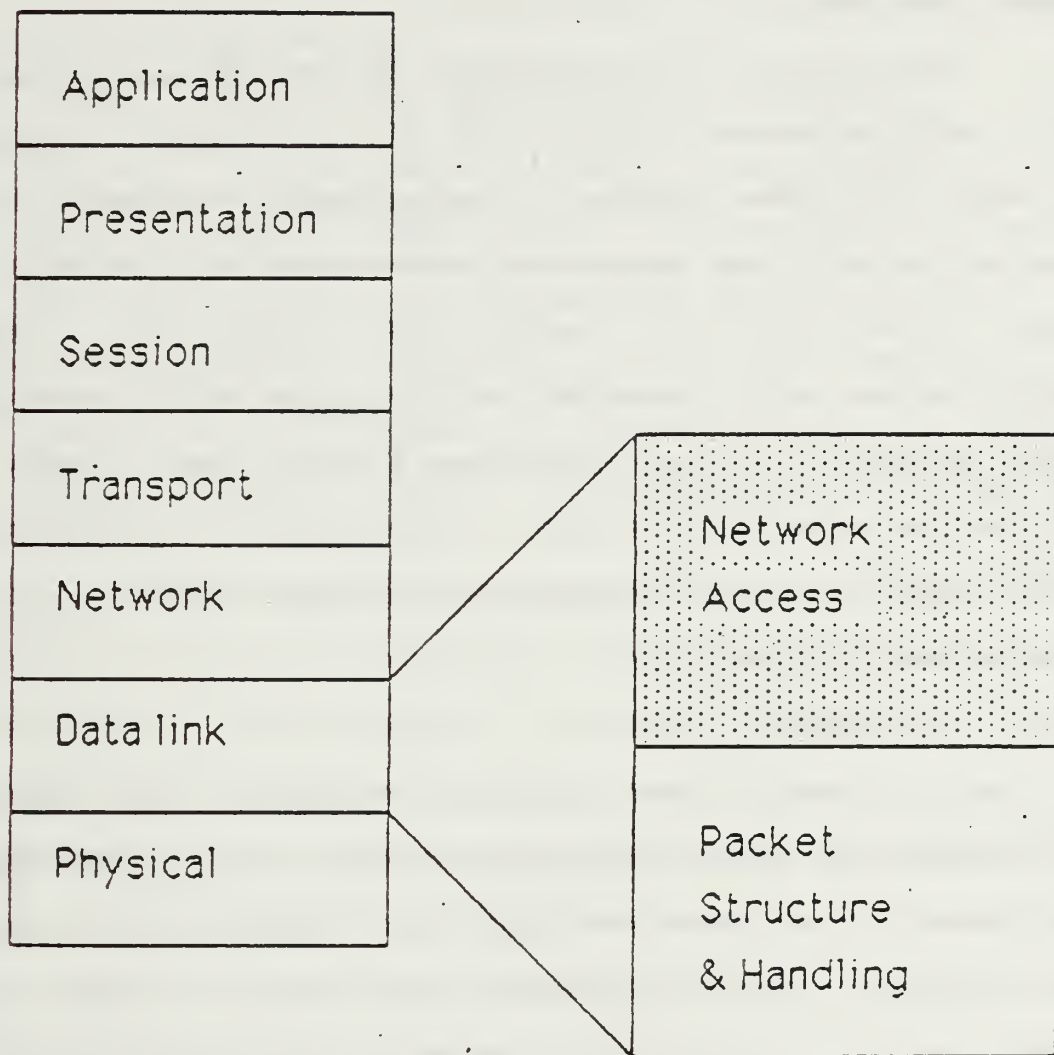
Figure 4.2   Data Link Division-Network Access.

C. THE PROBLEMS

The problems of network access methods in sea service communications arise from three big categories which we will examine separately:

1. Invalidation of Conventional Network Access Methods

All networks consist of a collection of stations that must share the network's transmission capacity. Some means of controlling access to the transmission medium is needed, so two particular devices can exchange data. In this subsection, we will describe carrier sense multiple access (CSMA) and token access techniques which seem likely to dominate the marketplace. Also, an explanation will be given on the question "why we cannot use these methods in sea service communications.

a. CSMA/CD

A station that wishes to transmit, first listens to the medium to detect if another station is transmitting. This usually involves sensing the presence of a carrier signal. If the station detects that the medium is idle, then it may transmit. Otherwise, the station has to wait for some period of time before it tries again to detect the status of the medium. With Carrier Sense Multiple Access with Collision Detection (CSMA/CD), three types of algorithm are needed to specify what a station should do if the medium is found to be busy [Ref. 8].

* Nonpersistent: If the channel is busy, the station waits a random time drawn from a probability distri-

bution (the transmission delay), before sensing the channel again. The use of random retransmission times reduces the probability of collisions. The advantage is that even if more than one station is waiting to transmit,it is likely that each will back off for varying times and hence avoid another collision. However, it is likely there will be some wasted idle time following a prior transmission.

*   1-Persistent: If the medium is busy, continue to listen until the channel is sensed idle, then transmit immediately. If there is a collision (determined by a lack of acknowledgment), wait a random amount of time and then try again. Unfortunately, if more than one station is waiting to transmit, there will be a collision since multiple messages are transmitted simultaneously.

*   P-Persistent: If the medium is busy, the station continues to listen until the channel is idle, then it transmits with a probability p. With probability (1-p) it waits for a fixed time, then senses the channel again. This algorithm attempts, to minimize idle time and collisions.

As we saw from the above algorithms, they do not completely prevent collisions. There is a situation where two station will detect an idle channel and begin transmitting simultaneously. To avoid this problem there exist some systems that use error-detection mechanisms. Some other systems detect collisions immediately by monitoring the channel during the transmission and discard the transmission when a collision is detected.

Stations in a long haul, HF network, cannot be assumed to be able to hear each other. In this case we can assume that all stations can hear the communications station (at least most of the time). This invalidates the use of CSMA schemes to manage access to the sea service communications. A more primitive network access scheme than

83

carrier sense is collision detection (ALOHA). But, collision detection is too wasteful of an already severely constricted bandwidth to be considered as a controlling access method. Additionally, collision detection under an offerred load greater than the channel capacity is a fatal drawback for sea service communications.

b. Token Models

This is a relatively new technique for controlling access to a broadcast medium. The token technique is more complex than CSMA/CD. There are two token techniques, token bus or tree and token ring.

(1) **Token bus or tree technique**. For this technique the stations form a logical ring, which means that stations are assigned logical positions in an ordered sequence, with the last number of the sequence followed by the first. Each station in the medium knows the identity of the stations preceding and following it.

A control frame (a sequence of bits) known as a Token regulates the right of the stations to access the medium. The token frame contains a destination address. The station that receives the token is granted control of all the medium for a specified amount of time. During this time the station may transmit, poll a station, and receive responses. When the station is done, or time has expired, it passes the token on to the next station in logical sequence. This station now transmits. Non-Token-using stations are not

allowed to transmit, these stations can only respond to a poll or request for acknowledgement.

        (2) **Token ring technique**. This technique is based on the use of a single token that circulates around the ring when all stations are idle. A typical example of a token is an 8 bit pattern such as "01111111". A station that wishes to transmit must wait until it detects a token passing by. Then the token is changed from "free token" to "busy token". This can be done by changing the last bit of the token, for instance "01111111" to "01111110". The station then transmits a frame immediately following the busy token. [Ref. 5]

        There is now no free token on the ring, so other stations wishing to transmit must wait. The frame on the ring will make a round trip and be purged by the transmitting station. The transmitting station will insert a new free token on the ring when the station has completed transmission of its frame and the busy-token has returned to the station.

        When a transmitting station releases a new free token, the next station downstream with data to send will be able to catch the token and transmit.

        Again, because ships may not be able to hear each other, token passing is not an applicable network access technique either. If the token is passed via the

communications station, then the system becomes essentially a centrally controlled one.

2. <u>Physical Layer Considerations</u>

In the sea service HF communication links, full duplex simulation is difficult, if not impossible. Additionally, within the HF band, there are some problems that are theoretically possible to deal with at the physical level, but the solutions are more expensive than dealing with them at the logical link and network levels [Ref. 1]. These problems are specified as follow.

a. Requirement for Synchronous Equipment

Most conventional networks are operated under an asynchronous environment where reversal of the channel (from send to receive) is quick and inexpensive. For synchronous equipments, synchronization preambles are required that make it expensive to reverse the channel (switch from receive to send).

But in sea service communications, especially when units are under tactical operation, encrypted messages are required. Once a network becomes a covered circuit, synchronous communications are imposed by most cryptographic devices, plus a synchronization requirement for synchronous modems. For example, if we use the VSQ-83 modem and KG-84 cryptographic devices, each one requires a synchronization consisting of 0.8 seconds or 1.6 seconds for each

transmission sequence. One 256 byte packet transmitted at 2400 baud requires 0.85 seconds (we use ASCII model).

$$T = \frac{256 * 8}{2400} = 0.85 \text{ sec}$$

Thus this arbitrary choice of parameter would result in nearly twice as much channel time taken up in synchronization than in transmitting data. This situation becomes considerably worse by using different types of modems. There are some types of modems which use interleaving or spread a message over a long period of time, to combat fading errors. While these modems improve the quality of a continuous bit stream, this can potentially degrade a logically bursty communications system.

For the above reasons, our purpose is to construct the over all system so that at the physical layer reversal will be minimized. That means the physical layer bit stream is as continuous as practical, regardless of the logical burstiness at higher levels. A practical solution to this problem is to bunch several packets together.

This solution is implemented by X.25 protocol by allowing the ending flag byte of a packet to serve as the leading flag byte of the next packet. The physical layer equipment does not lose synchronization, because a sequence of flag bytes is used as spacers between packets. This

87

method is the first step toward making a logically bursty circuit appears as continuous to the physical level.

This synchronization method is an argument for long access periods for each station, long enough to transmit all traffic in the queue. The opposing consideration is to allow access to all stations. The station is not monopolized the channel until clear all his traffic in the queue. These considerations are alternatives between throughput and grade of service. The requirement to operate high precedence traffic requires a degree of interruptability.

b.   Full Duplex Inhibitation

There are several other considerations, which continue to observe the principle that ships cannot transmit and receive at the same time. Since these reasons have been examined in previous chapter, here they are merely mentioned with a brief explanation.

* Signal to noise ratio. This is the physical difficulty when receiving a faint signal in the presence of a strong physical transmitted signal (Noise). Because of the often poor signal to noise ratio, sea service communications require a synchronization preamble for the modem.

* EMCON. This situation is applied when stations are operated under tactical emission control (EMCON) considerations.

* Transceivers. Most equipments are packaged with transmitter and receiver in the same box, known as a tranceiver. In this condition, it is impossible to operate transmitter and receiver simultaneously.

* Hazard conditions. This includes some other reasons such as shipboard power failures, incompatibility with

other ship sensors and hazards of electromagnetic radiation to other ship equipments (ordnance).

c. Downward Multiplexing

In the case where a ship needs more capacity from one channel, then the system must provide this ship with more channels ganged together to cover the necessary bandwidth in aggregate. In the HF band, one controller must exist to control all ship's transmitters and preclude one channel transmitting while another is trying to receive.

As it is implied from above, the synchronization issue, which is link specific to HF, must be handled at this level of the reference model, rather than at the network level. This is done because at the network level the protocol should not be required to know what the dependencies are between links.

3. Flow Control

The utility of network level acknowledgment will be assumed in this chapter, since the reader of this thesis should be convinced by the arguments in the previous chapter. As we mentioned in the previous chapter, temporal decoupling is an implication of network level acknowledgment. This implication is important to the consideration of flow control mechanisms.

We are not going to examine each flow control mechanism, since it is not the purpose of this thesis. We just mention why the conventional flow control mechanisms cannot be used in sea service communications.

For the case of stop and wait protocol, it will not do for a ship to be able to receive one packet and then have the system stop until the ship acknowledges this packet. For the same reason the sliding window protocol (Go Back N) no longer works. It will not do for a ship to be able to receive eight packets and then have the system stop until the ship acknowledges those packets.

Selective repeat provides the only feasible approach. The only packets retransmitted are those that receive a NAK. On the other hand, the transmitter will require complex logic for enforcing it to transmit packets out of sequence. Also, the receiver must provide enough buffer capability to save Post-NAK packets until the error packet is retransmitted, and the required logic to insert the packet into the proper place in the sequence.

Another issue that we have already mentioned in a previous chapter is the implication of temporal decoupling. Conventional networks require prompt responses, while in sea service communications, this may not be practical in many situations. There is no imperative of the communications system itself that requires packet acknowledgement immediately. Therefore the response time should depend on the operation and content of the communication itself, not an exigency of the communications system.

D. NETWORK ACCESS ALGORITHMS

The remainder of this chapter deals with the synchronization issue, by examining and building a series of models at least flexible and robust enough to use in our HF system. During this full duplex, simplex polled circle and half duplex models will be examined. Before the polling systems examination we are going to give values to some variables, which will help us in the models' analysis. The values chosen are arbitrary, although there are some reasons for each one to be realistic. We will not represent the reality of each value, because this is not the purpose of this thesis, we will just mention the values of these variables.

* Data rate 2400 baud
* Packet size 256 bytes
* Cycle time 2 minute
* Network stations 20 ships
* Synch time 1.5 seconds
* Time for silent periods zero (0) seconds
* All packets are received correctly, no ARQ.

1. Full Duplex System

a. Description

In a full duplex system, the communications station and the ship must not be required to operate on the same frequency. We will explain this advantage later in this

91

chapter. Now, a description of system operation will be provided.

(1) **Step one. Polling the Network.** The communications station polls ship's network by sending a polling packet to each ship in turn. Each ship responds with a summary of its queue contents, for instance 200 bytes of Immediate 500 bytes of priority and 2000 bytes of Routine.

(2) **Step two. Balance Order List and Conversation.** The communications station balance the ships' queues and prepares the ships' sequence. Then it simply converses with each ship, at a time, in turn. The conversation would be in full duplex mode, meaning that the ship is responding as the communications station is sending its traffic. During this conversation both communications station and subject ship attempt to clear their queues. The cycle is terminated when an amount of time is over, and the communications station continues its operation on the next ship in the sequence. If there are any sent packets that are not acknowledged, then these packets are assumed lost and are queued for the next cycle. Silent periods are allocated in the cycle for new ships to enter the network or to get send a brief (one packet) high precedence message. The full duplex polling circle is illustrated in Figure 4.3.

b. Advantages

This system is very attractive because there exists a standard X.25 protocol that is designed to work for

92
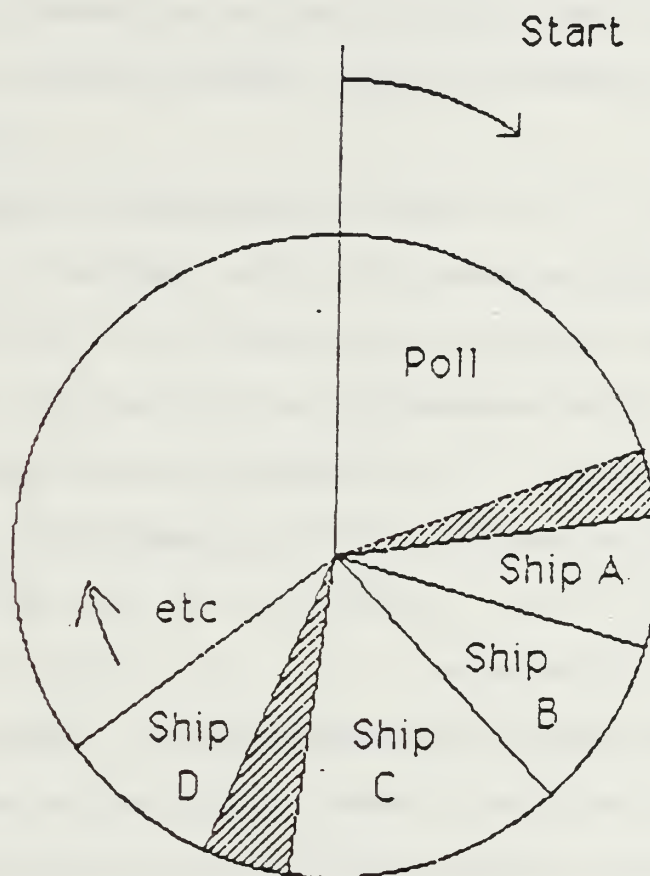
Figure 4.3   Full Duplex Polling Circle.

it. Its Go-Back-N error control algorithm with its sliding window remains useful.

Another advantage of this system is that it does not require the ship station to be sophisticated regarding network access. Each ship waits its sequence in the network until it is called by the communications station to transmit.

But, the biggest advantage to this system, as mentioned in the beginning of this section, is that all ships are not required to transmit on the same channel (frequency). If the communications station has the ability to change frequency in its transmitters and receivers, than it can respond to each ship's requirements by shifting to a new frequency.

c. Disadvantages

Full duplex communication is impossible in sea service. The ships cannot operate full duplex in the HF band for many reasons, as were mentioned in previous chapter.

In this system there is very close temporal coupling between sending and receiving. This is again difficult for those reasons we have described in the last chapter of downward multiplexing.

Another disadvantage with this system is that a ship must broadcast in order to receive. This is a against the normal operation of a ship able to receive passively. Also the collective address broadcasting which is very

94

effective in sea service communications will not work with this model. The reason is that a packet received by a ship cannot be acknowledged if the ship is not concurrently listen to the communications station.

A general conclusion is that full duplex models are not efficient and flexible enough to work in sea service communications.

2. A simplex polled circle

In this model both communications station and ships operate on the same frequency. Two modes can be distinguished for the simplex polled circle.

a. Basic Polled Circle

(1) Description. The algorithm of this access model is explained in the steps below which are also illustrated in Figure 4.4.

(a) Step one, Polling the Network. The communications station polls ships' network by sending a polling packet to each ship station in turn. Then, each ship responds to the polling packet by sending a summary report of its traffic queue contents.

(b) Step two, Organizing a Sequence Order List (SOL). The communications station collects all ships' responses, balances the ships' queues with its own traffic and organizes a broadcast schedule. The communications station then broadcast the SOL which gives each ship her turn to transmit in the network.
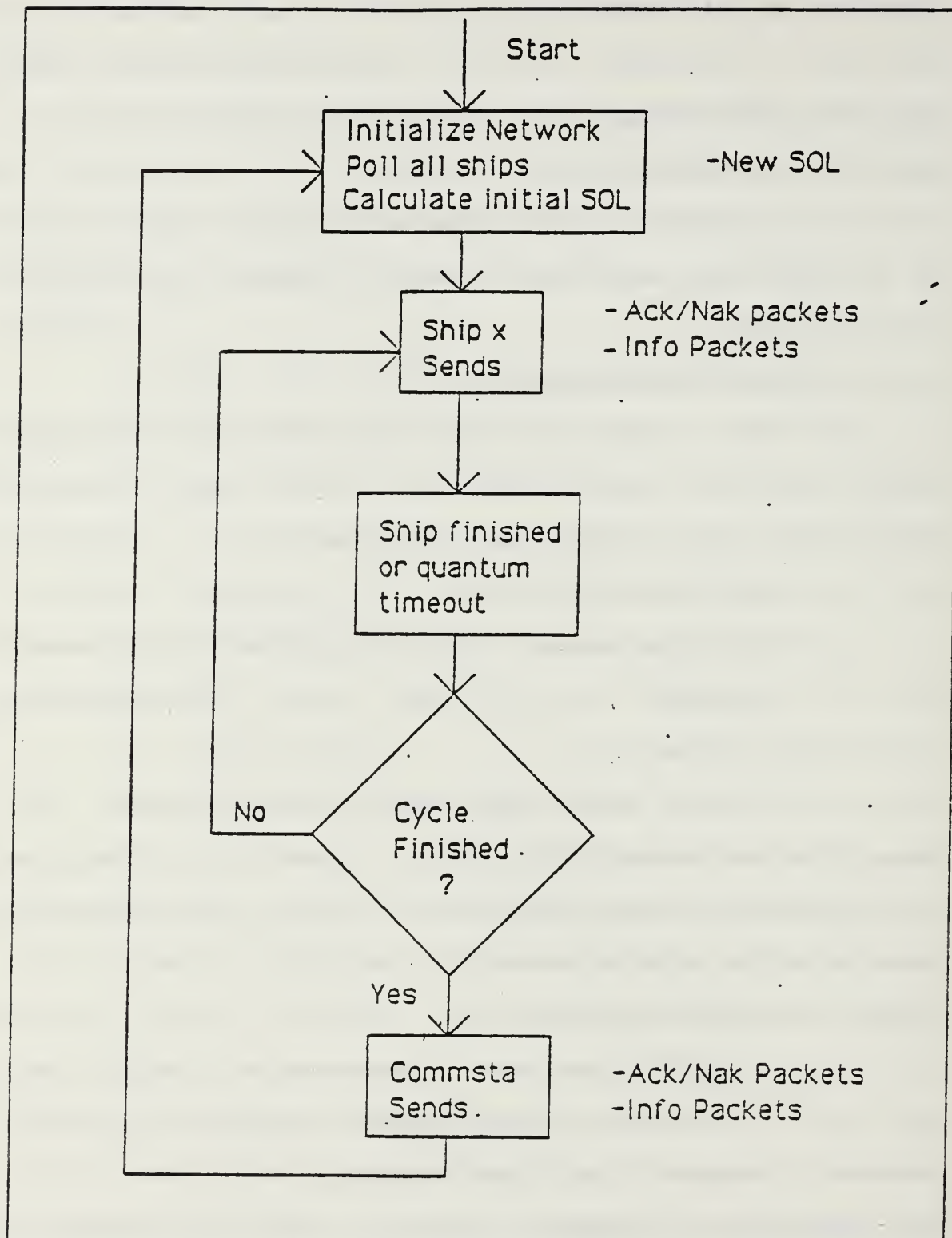
Figure 4.4   Basic Simplex Polling.

(c) Step three, Ships' Turn Transmission. During this step, the ships transmit their own outgoing traffic including any acknowledgments from the previous cycle. It must be noted that the cycle is time clocked, so ships are not required to hear each other.

(d) Step four, Communications Station Turn. The communications station turn comes again to send its traffic including acknowledgement packets for ship traffic. Any requests for repeats (NAKs) are also included in this step.

(e) Step five, Repetition. After the communications station turn, the cycle is finished and the next cycle is starts by the communications station starting with step one. The basic polled circle is depicted in Figure 4.5.

(2) Model's Analysis. Our purpose in model analysis is the synchronization issue since it is a link issue specific to HF. As was shown in the cycle description, the communications station will have to transmit its synch three times. One per ship in the polling sequence, one for SOL transmission and one for its traffic. On the other hand, each ship has to transmit its synch twice per cycle. One when it responds to the poll and one when it sends its traffic. This results in about 93 seconds, of the two minutes (120 seconds) cycle time, for synchronization

97
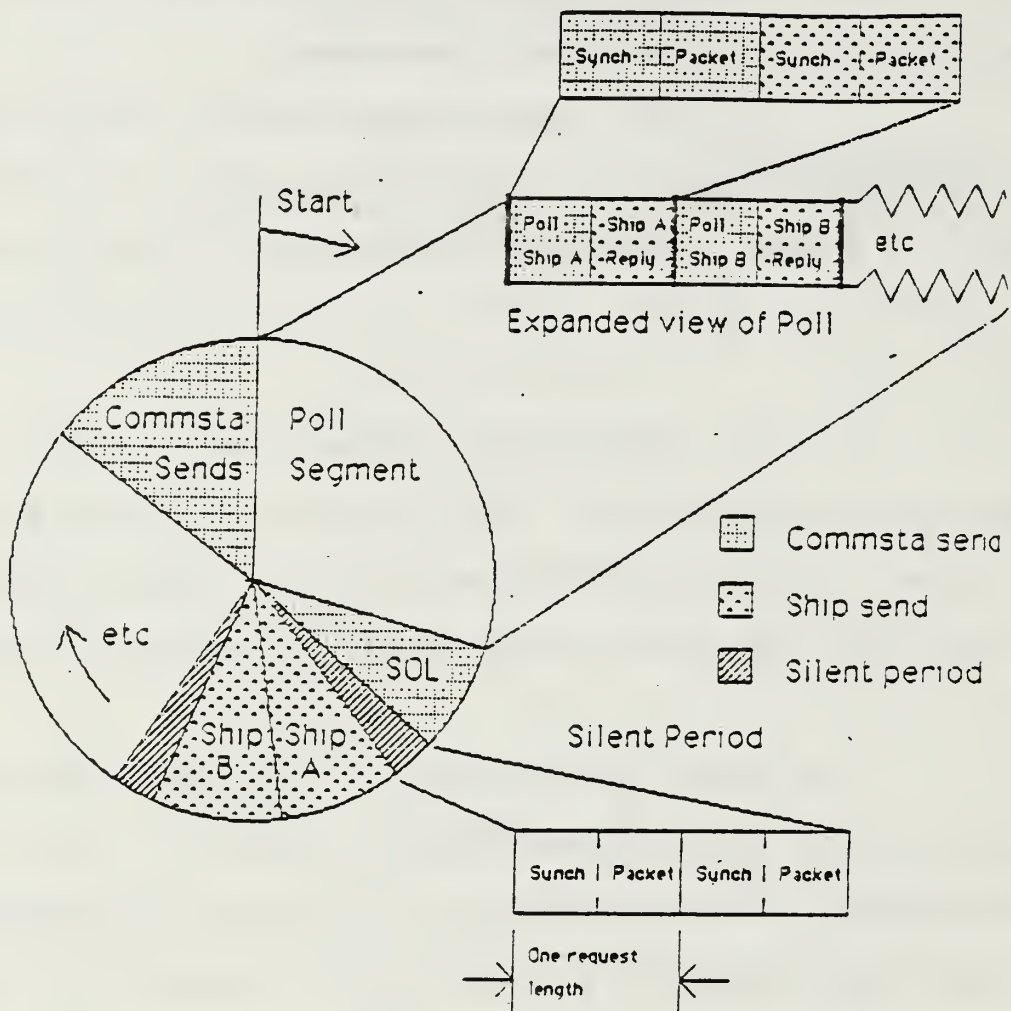
Figure 4.5   Basic Simplex Polling Circle.

requirements. This is more than 3/4 of the cycle time and so it is not effective.

b. Revised Polled Circle

This is essentially a simplex polled circle. The main advantage of this model is that it eliminates some of the synchronization overhead.

(1) Description. The algorithm of this model follows the below steps, which are also illustrated in Figure 4.6.

(a) Step one, Polling the Network. The communications station polls the network by sending a polling packet to each ship in turn, and each ship responds to the communications station polls. This is exactly the same procedure as with the basic polled circle.

(b) Step two, Organizing a Sequence Order List (SOL). The communications station selects all ships' responses, balances them with its own traffic and broadcasts a schedule (SOL) which gives each ship its turn to transmit.

(c) Step three, Communication Station Transmit. During this step, the communication station transmits its traffic immediately after the SOL broadcast. The advantage of this model is that it reduces the synchronization overhead by transmitting the SOL and communication station traffic together. Also, this step includes acknowledgements from ship traffic in the previous cycle.
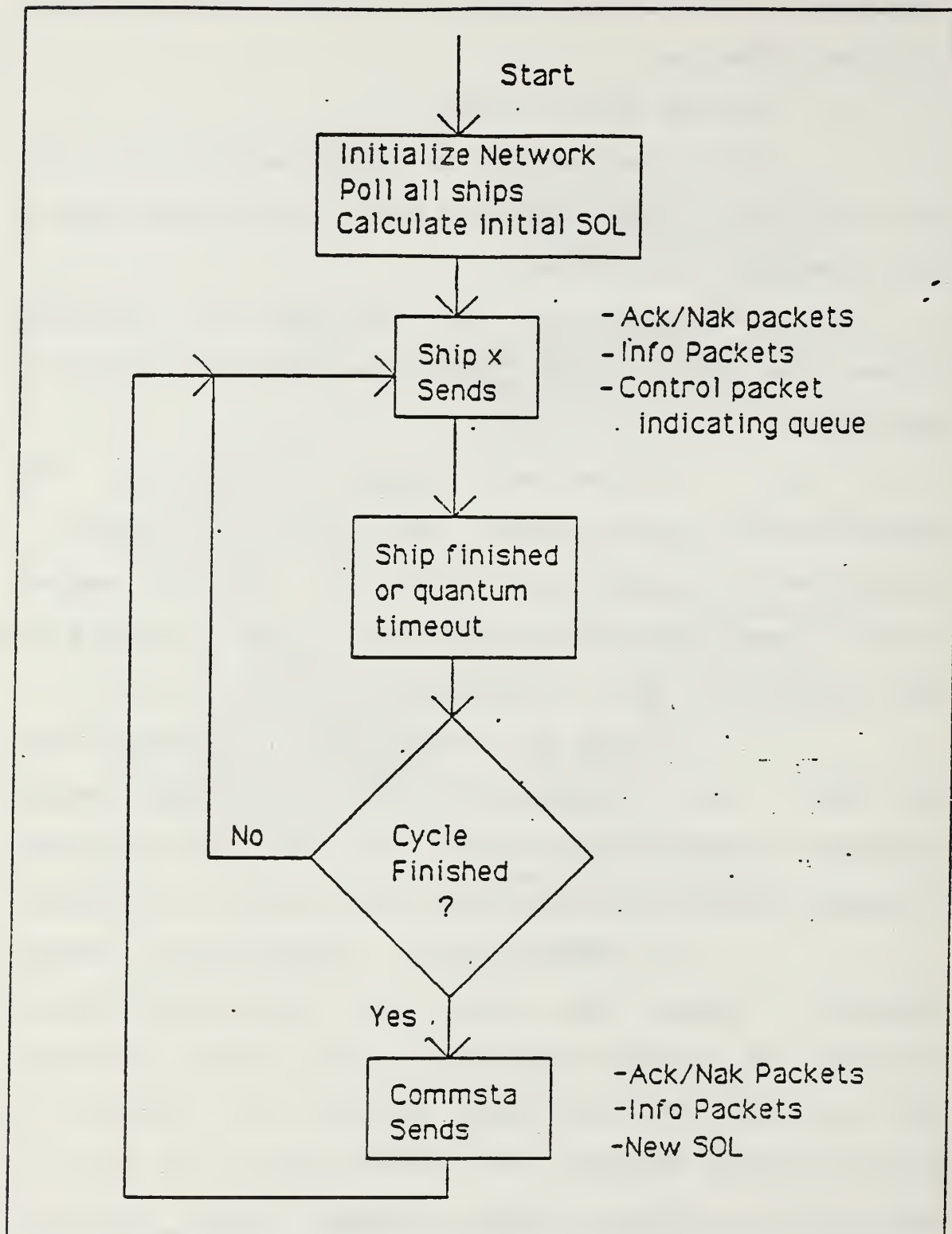
Figure 4.6   Revised Simplex Polling.

(d) Step four, Ships' Turn Transmission. This includes ships' traffic transmission with acknowledgements from the previous cycle. At the end of each ship transmission, a polling packet is sent to the communications station indicating the amount of traffic remaining in each ship queue.

(e) Step five, Repetition. After ships' transmission the cycle is finished and the next is started. The advantages of this model is that the polling cycle is not required, because the data for the next SOL was gathered in step 3, and the communications station starts the next cycle from step two. The revised simplex polling circle is illustrated in Figure 4.7.

(2) Model Analysis. Since our purpose in analysis is the synchronization issue, a calculation of overhead synchronization will take place, using the values mentioned at the beginning of the chapter. In each cycle of this model, the communications station will have to transmit its synch one time only during the polling network and transmit steps. On the other hand, each ship has to transmit its synch once when sending their traffic. So, synchronization time is reduced to 31.5 seconds of a two minutes time cycle. This means that the synchronization overhead is about 26% or 1/4 of the cycle time.

A better indication will be to calculate the number of one page messages which could be sent over the
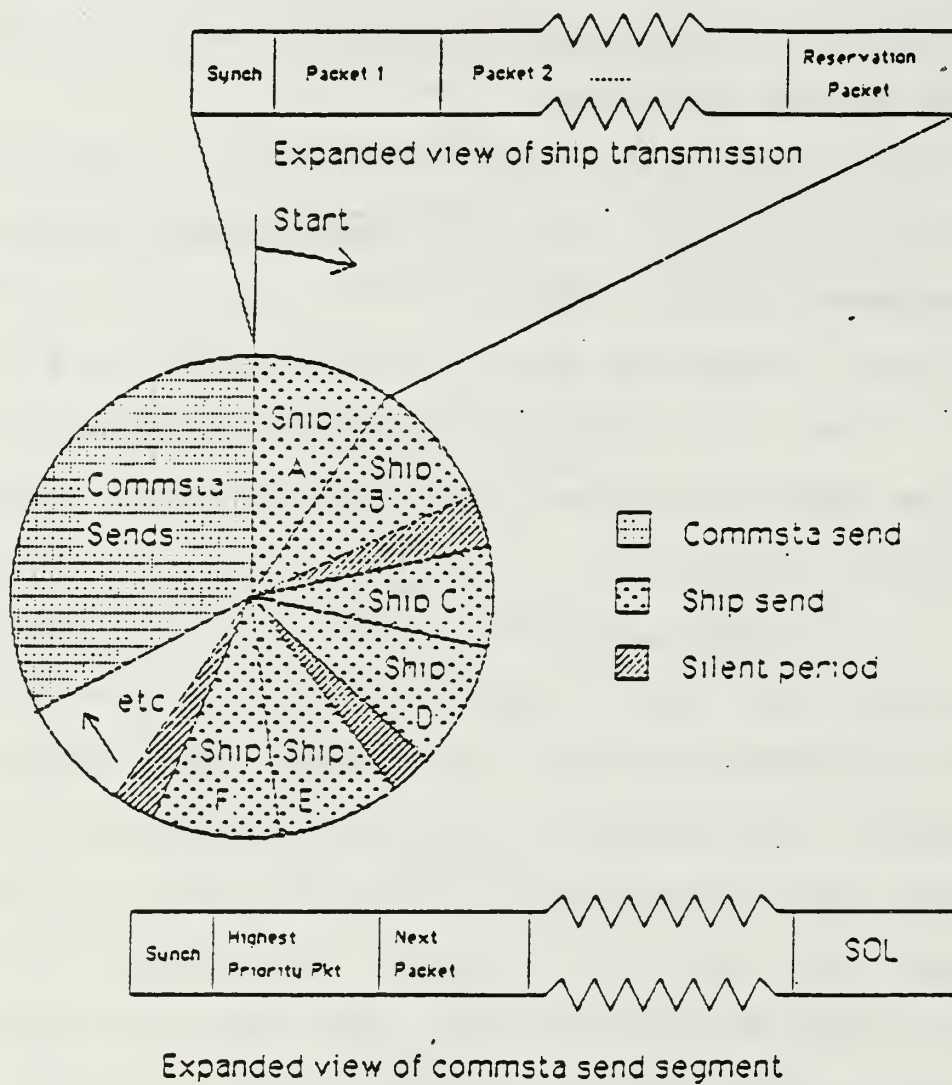
Figure 4.7   Revised Simplex Polling Circle.

link in the two minutes cycle time. If the communications system can operate at 2400 baud during the remaining 88.5 seconds of the cycle, approximately 27K bytes could be carried over the network. A one page message covers about 2K bytes. Then, the calculation results in approximately 15 naval one page messages transmitted over the link. This is an efficient result.

However this model has a disadvantage, due to the slight lag time in the queue management, as data added in the queue will not have been accounted for in the communications station poll. But, this problem is not serious if the ship has included in its polling response all the immediate and priority precedence packets added to the queue during the lag time are placed at the top of the queue and first out in the next cycle. Now if two or three cycles elapse until the queue is cleared, this delay time is not consequential. The sacrifice in grade of service is gained in increased throughput.

(3) <u>A deeper Analysis.</u> This is an analysis that goes further into the revised simplex polling circle model and examines issues such as silent periods, full period terminations, missing SOL, variations of service and throughput and grade of service considerations.

(a) Silent periods. With the model described above, a ship wishing to enter the network cannot since there is not an opening. So, the cycle is modified.

103

The communications station, before broadcasting SOL, takes into account some silent periods allocated in the cycle time where none of the existing participants may transmit.

The main purpose of the silent periods is to permit a new ship, which wishes to enter the net, to send a net entry packet during these silent periods. The net entry packet contains the same information as a packet that is polled for by the communications station, the summary of its content queue traffic. If more than one ship tries to enter the net of the same time, then collisions occur. This can be handled by using a collision detection system.

Another purpose of using silent periods is to allow any station to enter the network and transmit an emergency or high precedence packet (flash, for example, an enemy report) without waiting its turn in the SOL.

(b) Full Period Terminations. This is an extreme case where a particular channel is dedicated to service one ship during the entire cycle time. During the cycle the communications station and the ship exchange their queue traffic. If the channel is turned around in small time intervals, once per minute for example, then the time lag in the queue management as data that is added in the interim, will be tolerable and only negligible additional overhead is needed.

(c) Missing SOL. There are many reasons where a ship in the net fails to receive the SOL and so, it

does not know its scheduled sequence. In this case the ship must refrain from transmitting in the cycle. On the other hand, the communications station must allocates it some time in the succeeding cycle. After a number of cycles, the communications station can delete it from the SOL and its slot in the cycle allocated in favor of other ships. Some reasons for the ship to fail to transmit in a large number of cycles is that it suffer from damage or power failure or it may have entered EMCON unexpectedly.

(d) Variations in service. There are several cases where a ship may manage several services in the cycle by using control packets.

When an EMCON is effected the ship must not transmit during the EMCON period. That means it will wish to receive, but the communications station must not include it in the SOL until the ship reenters the net.

The ship requests an extra SOL time slice in every cycle, even though it does not have pending queue traffic, to cover anticipated future traffic. The ship avoids reentering the net when the traffic is ready and gains in transmitting time.

When the ship anticipates a large volume of traffic requiring use of more than one channel, then it may include a control packet on one network, initiating a login into another new network.

(e) **Throughput and grade of service considerations.** These depend on the number of silent periods in a cycle. If the number of silent periods is large then the less the throughput. But, what is a large number of silent periods in a cycle? Of course, that means only extremely high precedence traffic would get through with very little queue delay. We have two applicable cases in sea service communications as to how throughput and grade of service are related with silent periods.

* A surface ship communications network can be best worked with high level throughput. That means small and infrequent silent periods.

* A network for aircraft or submarines may not need high level throughput, but rapid access to the net is more imperative. This requires frequent silent periods and sort scheduled transmissions.

There is the service case where the network is to be used for large quantities of data. Then silent periods must be omitted entirely. From the above, a balance is needed between throughput and grade of service for better effectiveness. This balancing can be done by the operators at the communications station, since it changes with the situation.

Another factor that influences the trade off between throughput and grade of service is the cycle time. A longer cycle time increases throughput at the expense of grade of service. In this case the number of cycles in a period of time decreases while the synchronization overhead remains constant.

3. Half Duplex Model

The main characteristic of this model is the exchange of information between two communications stations on different channels. So, it is now possible for the communications station to use an HF channel, while ships use satellite channels, an advantage for ESM reasons that we have mentioned in previous chapters. Once a half duplex set up is in effect the multiple channels of the downward multiplexing concept are fully usable.

a. Description

This model can be considered as an expansion of the simplex description that adopts the advantages and avoids the disadvantages of full duplex. The algorithm of this model follows the bellow steps, which are also depicted in Figure 4.8.

(1) **Step one. Polling the network.** The communications station polls the network by sending a polling packet to each ship in turn. Each ship responds with a summary of its queue contents as before. The difference here is that the communications station is using a sending frequency where it is the only transmitter, while the ships use other frequencies to send their responses. This can be accomplished by announcing the network and permitting any station to login to it.

(2) **Step two. Organizing a Sequence Order (SOL).** In this step, the communications station selects all ships´

107
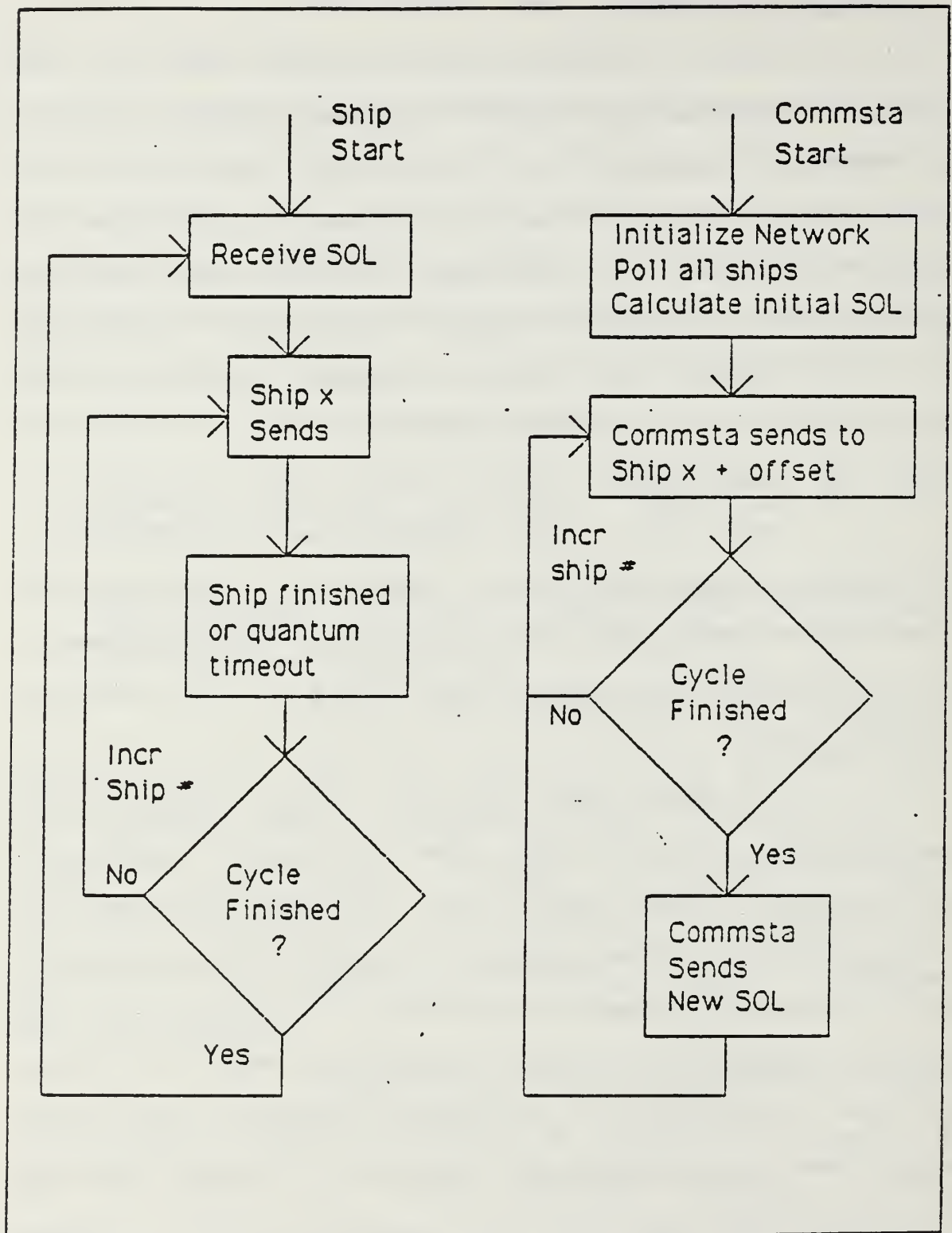
Figure 4.8   Half Duplex Polling.

responses, balances them without its own outgoing traffic, since they are sharing different channels. The communication station then broadcast the SOL that gives each ship her turn to transmit in the network.

The next two steps show the primary differences in half duplex. They are not consecutive, but are accomplished simultaneously.

(3) Step three, Ship's Turn Transmission. During this step, the ships transmit their own outgoing traffic including any acknowledgments from the previous cycle. The cycle is time-clocked, as before, so ships are not required to be able to hear each other. At the end of each ship's transmission, a polling packet is sent to the communications station indicating the amount of traffic remaining in her queue. Here, four service variations can be observed for each ship station.

The ship needs more space in the next cycle, since it has traffic remaining in her queue.

The second is that the ship wishes to remain in the cycle although it has exhausted her queue. This happens, because the ship is anticipating traffic and wishes to avoid the time required to reenter the network.

The third is that the ship can receive without an immediate requirement to transmit. This is compatible with EMCON requirements.

The last is that the ship goes out of the network. The silent periods are used when the ship decides to reenter. If there is any traffic during the period where the ship is out of the net the communications station stores that until the ship logs into the network.

(4) **Step four, Communication Station Transmit.** The communications station transmits its own outgoing traffic along with acknowledgements for ship traffic. But its transmission is at a different time than the ship is transmitting, since the traffic to a ship is timed. This can be easily accomplished, when more than two stations are on the net with roughly equal amounts of traffic, by offsetting the communications station transmit packet by about half of the cycle time. This would prevent interference in all but the most distorted schedules. This procedure is illustrated in Figure 4.9.(b).

(5) **Step five, Repetition.** After communications stations transmission the cycle is finished and the next is started. With this model also, the polling phase is not required, since the data for the next SOL was gathered in step 3, and the communications station starts the next cycle from step two. If the SOL is broadcast twice in a cycle and each ship is silent during at least one instance each ship can receive the SOL at least once in a cycle time.
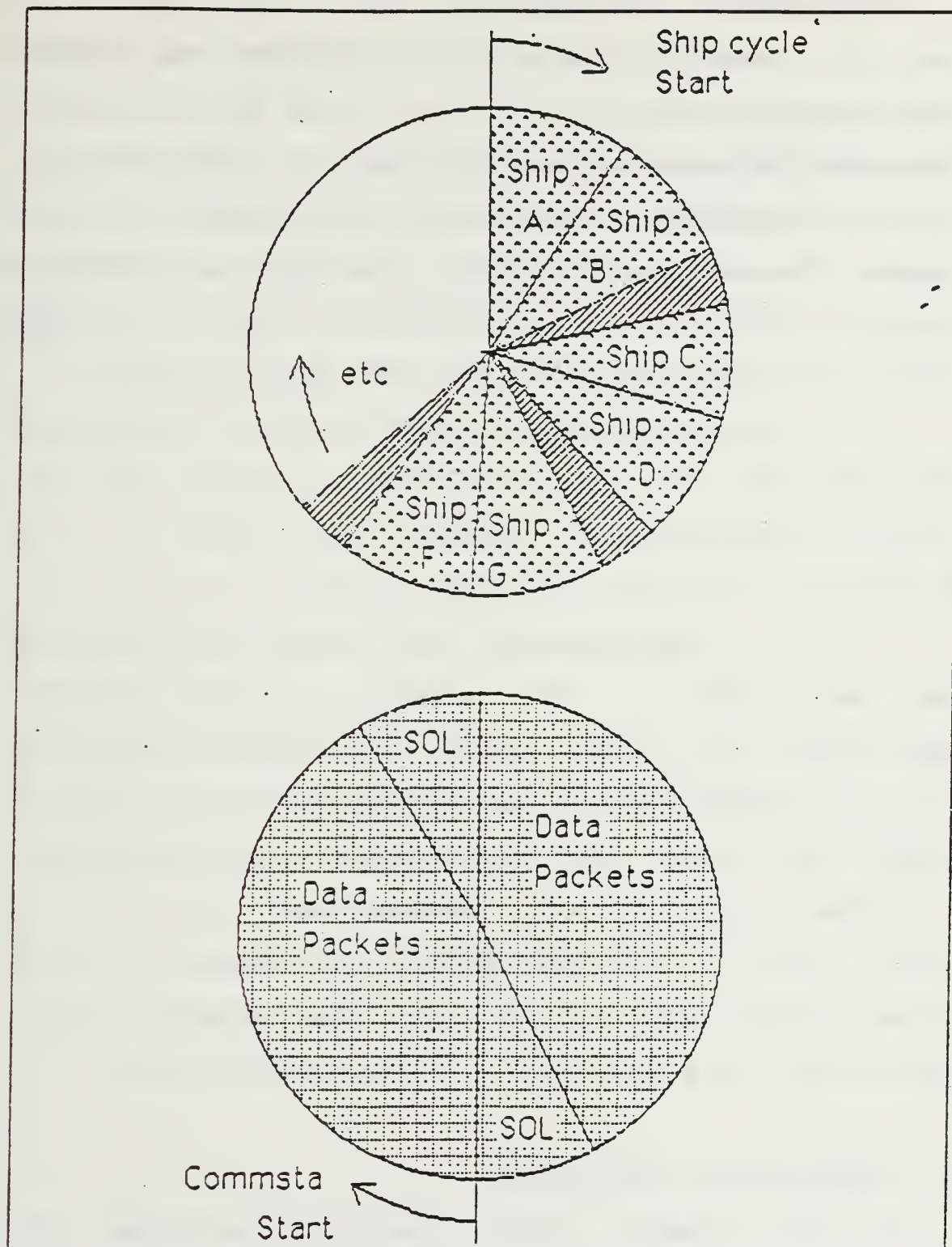
Figure 4.9   Half Duplex Polling Circle.

b. Model's Analysis

Again, our purpose is to calculate the required synchronization overhead in a cycle time. In each cycle of this model the communications station need not synchronize as it is transmitting continuously. For practical reasons, however, the communications station may need to synchronize once per cycle, in order to accommodate a new ship entering the net or to help ships that have lost synchronization.

On the other hand, each ship has to transmit its synch once per cycle when sending their traffic. Thus, the required synchronization overhead per cycle will be equivalent to the number of ships in the net.

If communications can proceed with the values that were stated at the beginning of this chapter, approximately 36K bytes should be carried in shore-ship direction and 27K bytes in the ship-shore direction since 30 seconds are needed for synchronization in a 120 seconds cycle time. Given that a one message page is 2K bytes in length, then 18 one page messages are transmitted by the communications station and 13.5 one page messages by the ships in the two minute cycle, a very good efficiency.

E. COMPARISON AND CONCLUSIONS

In this chapter, three practical algorithms were presented for network access control in an HF environment. The most attractive algorithms are revised polled circle a

half duplex since they require less synchronization overhead, get reasonable amounts of throughput, and are survivable in any band.

In particular, the half duplex attracts more advantages then the revised simplex and works well in a fully integrated, network-layer acknowledged, communications system.

V. LOGICAL LINK CONTROL LAYER

A. GENERAL

In the previous chapter, various network access methods were described. The result was that the half-duplex method should perform well in a fully integrated, network-layer acknowledgement system in sea service communications.

In this chapter we are going to deal with the logical link issues of sea service communications. These issues are found in the lower half of the Data Link layer, the upper HF, network access, was described in the previous chapter. This is illustrated in Figure 5.1. The sequence of layer descriptions requires that this layer must be concidered after network and network access problems were dispatched. This is because the feasibility of the architecture in this chapter depends mostly upon the support of network protocol and network access.

To begin this chapter, two primary characteristics of sea service communications must be considered. These characteristics are the physical layer and physical layer equipment which the sea service logical link architecture will accept and deal with. Later on, the nature of the problem will be considered and three groups of errors will be classified. Then, an attempt will be made to counter each of these classes of errors by presenting error control
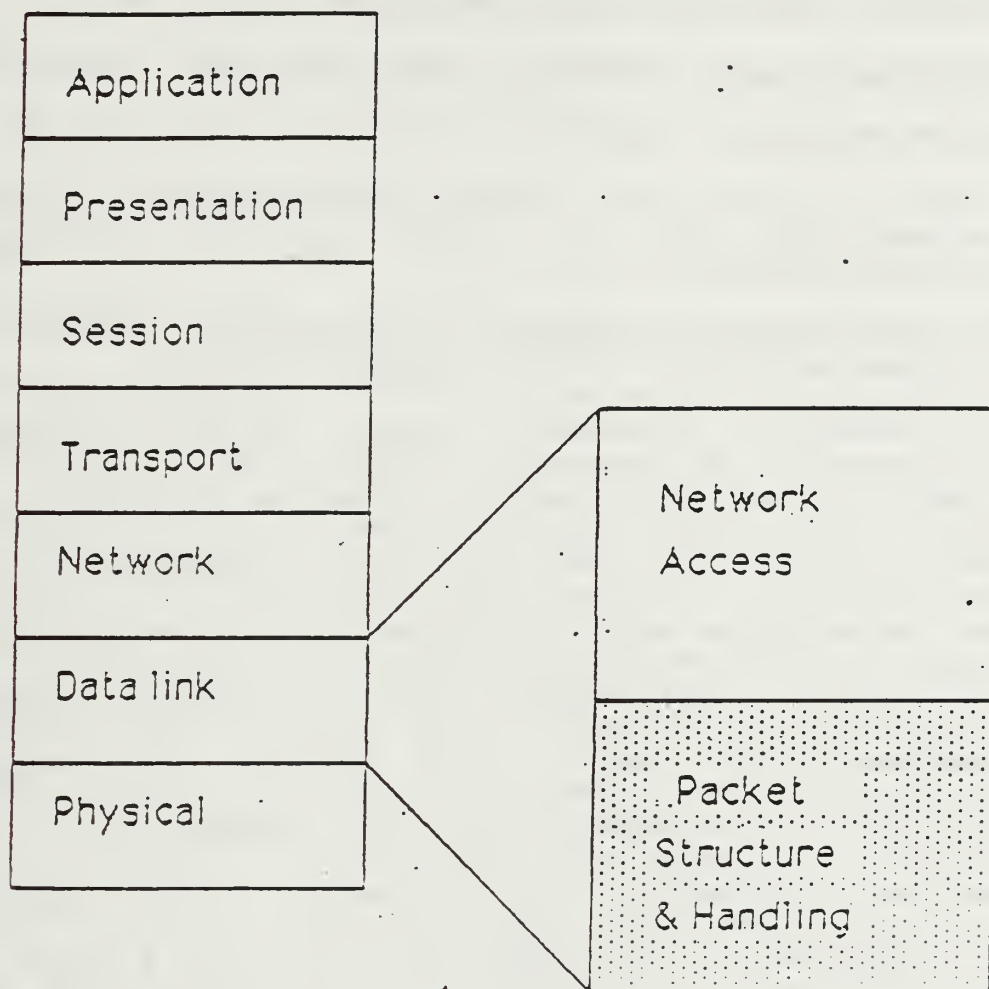
Figure 5.1   Data Link Layer Division-Packet Structure
and Handling.

methods in a bandwidth constricted environment. After that, data compression techniques will be presented to reduce the entropy of a message.

B. LOGICAL LINK LAYER CHARACTERISTICS

The functions typically associated with the data link layer are as follows [Ref. 4]:

*   Provide one or more service access points. A service access point (SAP) is a logical interface between two adjacent layers.

*   On transmission, assemble data into a packet with address and error control technique fields.

*   On reception, disassemble packet, perform address re-cognition and error control technique validation.

The logical link layer provides a connection protocol between two stations and an interface for a higher sublayer. That is, access to the network layer is provided by means of an interface to the Logical Link Control (LLC) sublayer. This layer is concerned with the transmission of data between two stations with no intermediate switching nodes, as is desirable in sea communications. At a minimum, this sublayer should perform those functions normally associated with:

*   Error Control: end-to-end error control and acknowled-gement. The link sublayer should guarantee error-free transmission.

*   Flow Control: end-to-end flow control.

In additional to the above logical link layer characteristics there are some other specific

characteristics of the HF environment which our logical link architecture must accept and deal with.

The first is concerned with the existing physical layer. The transmission medium in HF is the earth's atmosphere, especially the ionosphere layer. Obviously, there is not any method to control and change the ionosphere's characteristics or the physical way it reflects HF waves during their transmission.

The second deals with using the physical layer communications' equipments. Since the purpose of this thesis is to develop an architecture of sea service communications, the intention is to provide a framework to accommodate the existing equipments, as well as planed replacements, such as transmitters and receivers. Once the basic architecture has been provided, then the individual system's development can be upgraded only to that level without any requirement on the basic system as a whole. This means that changes can be made to the physical layer without any impact on the network and higher layers. This is done, because integration of various link functions is performed at this level, so changes are isolated to that link. The individual development of the link layer is influenced by the following factors.

*   The electronic engineering developments at that level.
*   Funding availability.
*   The mission of each unit.

In addition to the above factors, there is another that must be taken into account during the architecture development. Most military communications use coded circuis or link encryption, especially for operational purposes. This requires cryptographic devices which also requires synchronous transmission, as was described in the last chapter. So this characteristic is more important in the last chapter than in this chapter.

C. NATURE OF THE PROBLEM IN THE LINK LAYER

In the previous section we mentioned that the transmission medium for sea service communications is the ionosphere with HF waves. Also, we mentioned the characteristics of the link layer required for this environment. This section deals with two primary problems characteristic to the HF environment and concerned with the logical link layer. We classify the errors in three groups:

1. Narrow Bandwidth HF Channel

Each HF channel is 3KHz wide. This is illustrated in Table I which gives a general listing of frequency bands, their common designation, typical propagation conditions, and typical service assigned to each band.

A single HF narrowband channel in digital communications will carry, at best, between 1000(1K) and 10000(10K) baud. This capacity is much less than that of conventional network links by about three orders of

TABLE I

FREQUENCY BANDS [Ref. 9]

Frequency Bands	Designation	Propagation Characteristics	Typical Uses
3-30 KHz	Very low Frequency (VLF)	Ground Wave, low attenuation day and night, high atmospheric noise level.	Long-range navigation, submarine communication
30-300 KHz	Low frequency (LF)	Similar to VLF, slightly less reliable, absorption in daytime.	Long-range navigation and marine communication, radiobeacons
300-3000 KHz	Medium frequency (MF) .	Ground wave and night skywave, attenuation low at night and high in day, atmospheric noise.	Maritime radio directionfinding, and emergency frequencies, AM broadcasting.
3-30 MHz	High frequency (HF)	Ionspheric reflection varies with time of day, season and frequency, low atmospheric noise at 30 MHz.	Amateur radio, international broadcasting, military communication, long distance aircraft and ship communication, telephone, telegraph, facsimile.
30-300 MHz	Very high frequency (VHF)	Nearly line-of-sight propagation with scattering due to temperature inversions, cosmic noise.	VHF television, FM two-way radio, AM aircraft communication, aircraft navigational aids.

0.3-3 GHz	Ultra high frequency (UHF)	Line-of-sight propagation, cosmic noise.	UHF television, navigation aids radar, microwave links.

	Old	New	
0.5-1.0	VHF	C	
1.0-2.0	L	D	
2.0-3.0	S	E	

3-30 GHz	Super high frequency (SHF)	Line-of-sight propagation, rainfall attenuation above 10 GHz, atmospheric attenuation due to oxygen and water vapor, high water vapor absorption at 22.2 GHz.	Satellite communication, radar microwave links.

	Old	New	
3.0-4.0	S	F	
4.0-6.0	C	G	
6.0-8.0	C	H	
8.0-10.0	X	I	
10.0-12.4	X	J	
12.4-18.0	Kn	J	
18.0-20.0	K	J	
20.0-26.5	K	K	
26.5-40.0	Ka	K	

30-300 GHz	Extremely high frequency (EHF)	Same, high water vapor absorption at 183 GHz and oxygen absorption at 60-and 119 GHz.	Radar, satellite, experimental.
10^3-10^7 GHz	Infrared visible light, and ultraviolet.	Line-of-sight propagation.	Optical communications.

magnitude. As Table I shows [Ref. 9], the HF band is between 1 MHz and 30 MHz and is useful for low capacity, worldwide radio communications. That means that there is a 27MHz bandwidth available in the entire HF spectrum. In this spectrum, roughly a fifth is usable in sea service communications and available to many users.

The big difference in capacity between conventional network and sea service communications is illustrated in Figure 5.2. This depicts the cross section of two pipes which illustrates the magnitude of the problem. The big pipe represents a channel of a conventional network with a capacity measured on the order of 10^6 bits per second (bps). The small pipe represents an HF narrowband channel measured on the order of 10^3 bps, using modern modems that run in 1k to 10k baud and data compression (this will be explained later), for squeezing every bit to accomplish as much efficiency as possible.

2. High Noise Level

The second characteristic problem of the HF environment is the error rate. The error rate is on the order of 1 bit in 10^2 or 10^3 range for an HF channel. This big probability of error is due to HF channels suffer from high noise levels. So, the error rate in this case is about three orders of magnitude more than in a conventional network. In a conventional network, the error rate is on the order of 1 bit in 10^6 range.
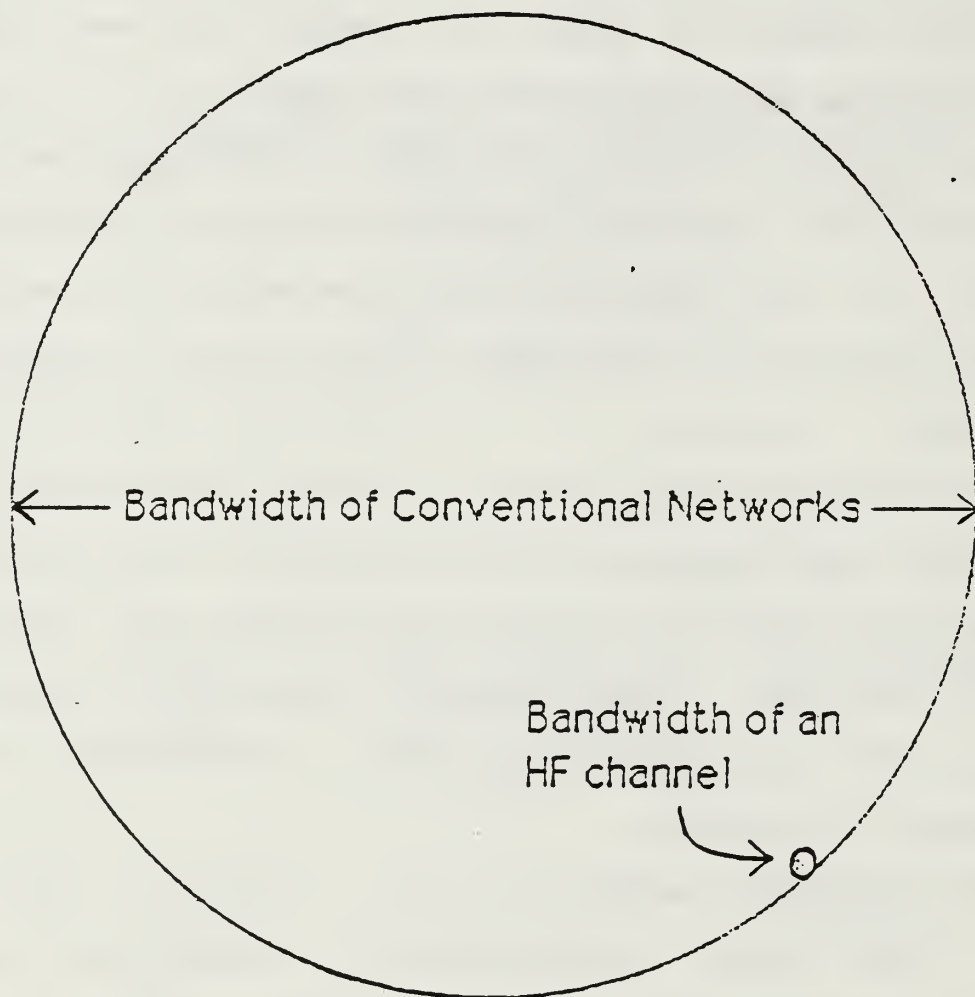
Figure 5.2   Bandwidth Magnitude of Conventional

Network and HF Channel.

122

The difference in error rate between a conventional network and an HF narrowband channel is illustrated in Figure 5.3. The cross section depicts again two pipes which represent the magnitude of these two channel error rates, but now in the opposite direction from the previous Figure 5.2.

3. Classification of errors in groups

The errors that are observed in HF radio band links are due to the HF environment, especially at the high noise level. These errors can be briefly classified into three groups according to their impact on communications at the digital level. [Ref. 1]

a. Burst Noise

This kind of noise is caused by lighting. If it happens during the transmission, it results in errors to the receiving message, ranging from 1 - 5 bits in length. The error length depends on burst intensity, duration, and on baud rate. This group includes some other anomalies in the ionosphere which result in essentially the same effect.

b. Short Term Fading

This group includes errors that persist longer than a few bits. These errors result in the corruption of a few bytes of data transmitted and create holes in packets. As a general rule, these errors corrupt parts of a packet and are more harmful than the previous error.

123
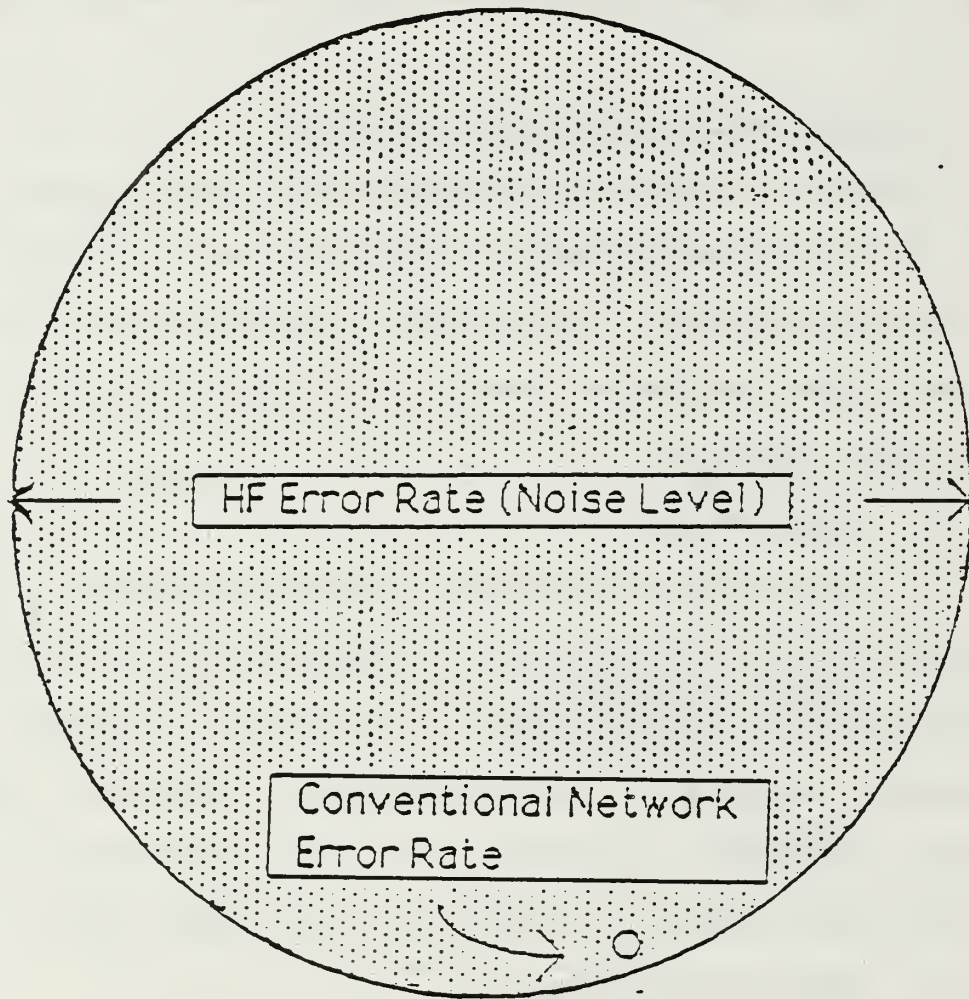
Figure 5.3   Error Rate Magnitude of HF Channel and

Conventional Network.

124

c. Long Term Fading

This group of errors includes those that result in complete los of packets. These errors are caused by the continuous rotation of the earth. Due to the earth's rotation, the two destination stations of the link are relocated relative to the ionospheric reflection and the frequency no longer works. So it is necessary to shift to another frequency. Missing packets' can be regained from the transport layer above the internet protocol.

Before leaving this subsection it is worth while to provide an overview of the ionosphere's anomalies. The ionosphere consists of the highest part of the atmosphere and includes a large number of loose electrons and positive ions. These loose electrons have the ability to reflect radio waves, which explains why stations can be heard at night. During daytime, long distance radio transmissions are not as good because there is too much ionization (too many electrons) in the lower ionosphere. These electrons absorb the radio waves on the way up to the reflecting layer.

From several kinds of measurements, we know that the ionosphere has huge diurnal variations, both in temperature and number of electrons. Also, the ionosphere becomes most active every eleven years, when the sun is disturbed by large solar storms, called sunspots. These storms, which consist of relatively cool gases in the solar atmosphere, appear as dark spots on the face of the sun.

Around the sunspots areas, bright flares of short duration appear and the outer portions of the solar atmosphere become extraordinarily hot. These flares also affect radio propagation on earth. A day or so after the appearance of solar flares, particles arrive from the sun which collide with particles of the ionosphere. These collisions excite the atoms, which then emit light. Thus, the northern and southern lights (the aurora borealis and aurora australis, respectively) usually appear a day or so after a major solar disturbance. [Ref. 10]

The logical link structure presented below attempts to counter each one of these classes of error by considering error and flow control.

D. ERROR CONTROL IN A BANDWIDTH CONSTRAINED CHANNEL

We mentioned in the logical link layer characteristics section that at a minimum, this link should perform two functions: error and flow control. In this section error control techniques will be considered.

The most common techniques for error control are based on two functions.

* Error detection. The mechanisms used to detect corruption are based on including redundant information within a message which allows the receiver to detect errors. Most popular techniques in conventional network are Parity Checks and Cyclic Redundancy Checks (CRC). To achieve further improvement the second technique (CRC) is used since it is very powerful and easily implemented. This technique will be presented later.

126

* **Automatic Repeat Request (ARQ).** When an error is de-
  tected, the receiver requests the sender to retransmit
  a corrupted packet. This algorithm is perfectly effe-
  effective in assuring error free reception, but requi-
  res adequate capacity to accommodate all errored packet
  retransmissions. If the capacity of our ship-shore
  physical layer is adequate for the communications task,
  this technique is sufficient. Unfortunately, the HF
  band suffers from narrow bandwidth, so a better error
  control technique must be developed for assuring error
  free reception of data.

1. <u>Cyclic Redundancy Checks (CRC)</u>

This is one of the most efficient algorithms for
error detection because it gives better error detection
capability with less redundancy.

The procedure can be explained as follow. Given a k-
bit packet or frame, the transmitter generates an n-bit
sequence, know as (frame check sequence) which is divisible
by some predetermined number. The receiver then divides the
incoming packet or frame by the same number and, if there is
no remainder, assumes that there was no error. To clarify
the above, the procedure can presented in several ways.

* Modulo 2 arithmetic

* Polynomial

* Shift registers and exclusive-or gates

In order to explain the two first cases, the
transmitter treats a message as a binary number (or
polynomial) which is divided, using modulo 2 arithmetic, by
a suitable binary number (generator polynomial). The
remainder forms check digits which are appended to the
packet or frame. This is equivalent to adding in the

remainder. On the receiver side a similar division is performed using the same generator polynomial. If there are no errors in the incoming data, the remainder will be zero.

For example, a 16-bit generator polynomial gives a 16-bit CRC code which is an overhead of only 1.6% in a 128-character message. A suitable r-bit polynomial gives the following error detection [Ref. 8].

* All single-bit errors

* All 2-bit errors

* All odd number of bits in error

* All error bursts of less than r+1 bits

* $1-(0,5)^{r-1}$ is the probability of detecting a burst of r+1 bits.

* $1-(0,5)^{r}$ is the probability of detecting a burst greater then r+1 bits.

Thus for a 16-bit polynomial, the probability of an undetected error for bursts greater than 17-bits is $1.5*10^{-5}$. Although the CRC checks are low and expensive to perform by software, they are available to perform error detection and are the most commonly used in conventional networks.

This ARQ algorithm is very effective at pure detection, it can declare if a packet is with or without error, but cannot determine how many errors are present in a packet. So, the CRC algorithm's decision is a binary one, either there are or there are not errors.

128

2. Error-Correcting Codes

This subsection is going to describe some methods of error control which will allow us to make our system more efficient, without sacrificing any effectiveness.

a. Automatic Repeat Request (ARQ)

As we mentioned above, the ARQ technique is very efficient when the ship-shore physical layer is adequate for the communications task. Since the purpose of this thesis is an architecture development, we are not going to describe ARQ techniques, but we refer to these and apply them to the ship-shore communications system.

Three versions of ARQ are in popular use.

* Stop-and-wait ARQ

* Go-back-N continuous ARQ

* Selective-repeat continuous ARQ

From these techniques, the Stop-and-wait as well as sliding window (Go-back-N) no longer work, they are not appliable to ships. A ship cannot receive one (in the case of stop-and-wait) or eight (in the case of go-back-N) packets and then stop the system until the ship acknowledges these packets. The only feasible approach is selective repeat.

Also, the basic ARQ system can be optimized. Messages are not sent as a whole, they are broken up into packets in order to optimize packet size and the medium. But the medium in sea service communications changes constantly,

if more capacity is required, so the packet size must be adjusted to account for changing error rate. During this thesis we are not going to present a balance between errors and packet sizes, rather the architecture to control this.

b. Forward Error Correction (FEC)

In addition to error-detecting codes, there are error-correcting codes. Error-correcting codes are referred to as forward error correction to indicate that the receiver, on its own, is correcting the errors. Retransmission modes, in contrast, are referred to as backward error detection, because the receiver feeds back information to the transmitter, which in turn retransmits those data which were found to be in error. So, forward error correction is a method of detecting and correcting errors without requiring retransmission of the errored data. This link level function increases the signal to noise ratio (S/N) at the physical level.

An error-correcting code is calculated from the bits to be transmitted and is then added to the transmission. To achieve acceptable levels of error correction, the length of the code must be about the same as the length of the data, reducing the effective data rate by 50%. The resultant undetected error rate with a code of this relative length is about 1 in 10^2 or 10^3 range.

This error correction can theoretically manage all errors, but its provision in the system rapidly

increases the sacrificed capacity required to get the benefits of it. Consequently, forward error correction can combat only burst errors in the range 1-5 bits in length.

Two techniques deal with the error correction scheme in this subsection. The first is concerned with adding bits in the errored data stream.

The effect of forward error correction in this case is twofold. The first is at the data layer, where this correction adds bits to the error stream, in order to allow a receiver to deduce which bits are transmitted in error and correct them. The second is at the physical layer. The result of adding bits to the data stream is to increase the overhead, which in turn requires more channel capacity. For, example, if one correction bit is used for every errored data bit, then the channel capacity is halved. Unfortunately, this narrows the physical layer bandwidth.

Forward error correction is less effective in error detection schemes, but its main advantage is the ability to localize the error and correct it. It is contrasted with the ARQ error detection schemes as mentioned above.

The second technique in an error correction scheme deals with interleaving of bits in the waveform to aid in correcting burst errors. This is done by separating the physical adjacency (sending sequence) and the logical adjacency (where they fit in the message). For example, if

131

we have a burst error that consists of three corrupted bits, they can be decomposed into three-one bit corrections and each one can be corrected individually. This is a good technique, but it needs to reverse the line for each individual error with all its disadvantages, such as overhead and synchronization preambles. For example, in a half duplex algorithm which is best appliable to sea service communications, an interleaving scheme will cause little effect on the shore-ship link, but a more substantial cost on ship-shore links with multiple ships.

Since the HF environment suffers from narrow bandwidth, forward error correction cannot be simply applied. The result is that this correction will be likely to detect and correct only burst errors that consist of 1-5 bits in length and will be less effective in handling longer errors. The forward error correction technique is handled by the feed back system, as with ARQ. This requires the receiver to package its reception diagnostic information into a control packet which is included with ACKs and NAKs and is sent to the transmitter for further actions.

c. Majority Voting

Majority voting is a hybrid method of error correction. It consists of forward and backward error correction methods used simultaneously. In the simplest case data is retransmitted several times and the received data is

compared for equivalence. Its particular applicability is in the HF environment for controlling short term errors.

Majority voting techniques are is theoretically quite simple. Data to be majority voted must be sent an odd number of times and at least three times. The odd number of times is required to exclude tie votes. The transmissions can be made either three times on the same frequency or on three separate frequencies. The number of transmissions primarily depends upon the level of noise on the channel.

An example will be presented for better understanding of majority voting theory. In this example a sentence will be taken into account as a packet which is received incorrectly three times. Each character in this example is transmitted correctly at least twice. Errors that occur only one time can be corrected. The majority voting result in this particular example is as follow.

```
shar-?=opa rokt.s svetcking natwapk
>hip=shore packet wwitkhang aetwork
sdip_sh're packet swigching nevjorw
----------------------------------------
ship-shore packet switching network
```

Another view is represented in the illustration of Figure 5.4, which depicts a packet by majority voting with fades in reception. The vote in a computerized system would be done by each bit, since the bit is the transmission unit.

This technique has some unique advantages. First, it can effectively correct packets with fade holes in them. This is a short term error which the forward error correction is not able to correct.

Second, the majority voter does not need any overhead when it is applied in the communication systems. Packets are only sent to it when they are received in error and require retransmission.

Third, not all stations in a network need be equipped with majority voters units. Of course the stations without majority voter require more repeats to receive a correct packet, but a mix of voter equipped and unequipped stations on a network can work well together.

This techniques requires· large buffers to accommodate a great number of damaged packets. This must not be considered as a disadvantage because of todays inexpensive computer memory and the fact that programming required to implement a majority voter is straight forward.

d. Majority voting in Packet Networks

Here, a procedure will be developed which uses majority voting within a packet network. The system verifies the packet in the packet receiver by using ARQ error control technique.

Step one, the damaged packet if detected in the receiver, is driven forward to the majority voter and is stored there until its next retransmission. If the
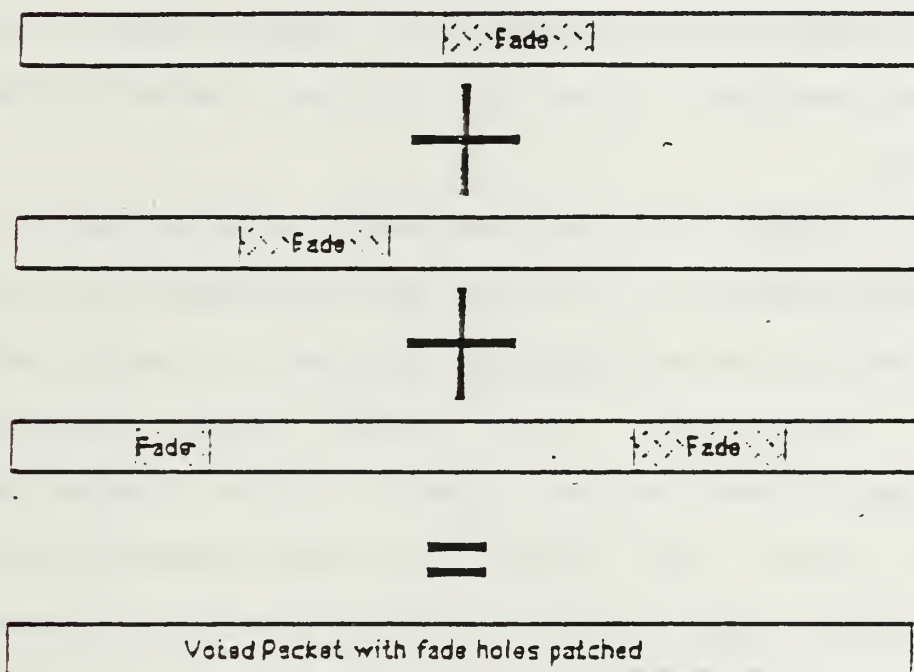
Figure 5.4   Fade Error Correction with Majority Voting.

135

subsequent retransmission returns a correct packet, then the majority voter discards the damaged stored packet. This procedure is opposite of the conventional network where the damaged packets were discarded by the receiver.

Step two, the majority voter gets three retransmissions of the damaged packet. Now, it has the necessary material required for its job. It votes on the three retransmissions, creates a new packet which is sent to the packet receiver. The packet receiver checks this packet for errors.

Step three, if the packet receiver decides that the received packet is correct, the procedure is continued and the majority voter discards its copy of damaged packets.

Step four, if the packet receiver decides that the received packet is not correct, it is retained by the majority voter, as closer to being correct and the retransmissions are repeated. This loop is started then from the beginning, step one.

An illustration of the majority voter's algorithm is depicted in Figure 5.5.

During this algorithm majority voting only takes place when the other methods have failed to correct all errors. The receiver is able to respond to the inability of the majority voter to correct a packet and to the bit error rate in one of the following ways.
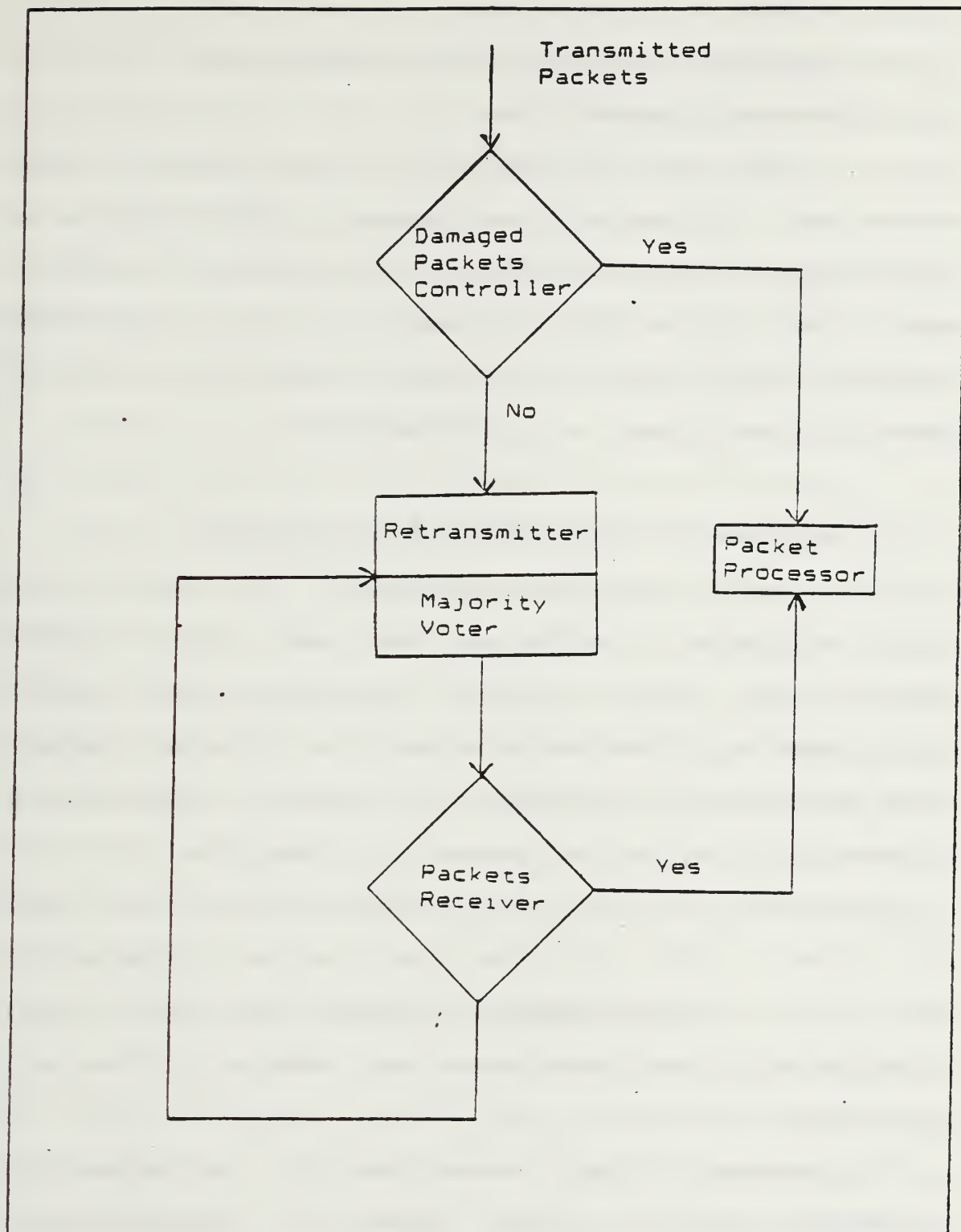
Figure 5.4   Majority Voter's Algorithm.

137

* A decrease in the flow rate

* An increase in the error controlling coding

* A decrease in packet size

       The general result of this section is that conventional Automatic Repeat Request (ARQ) technique in combination with majority voting can be used to correct errors due to the HF environment. Also, forward error correction can be used to increase throughput in the HF ·channel by sacrificing necessary bandwidth.

E. FLOW CONTROL AND DATA COMPRESSION TECHNIQUES

Flow control prevents overloading the capacity of a particular link or overflowing the input buffers at the receiver. There are a number of techniques which directly control whether a station is allowed to transmit a packet which were work in our system. The excited reader may wish to consult the references for sources of each one.

Our interest is turned to the capacity of our particular link, since our HF environment has a narrow bandwidth. So, techniques to increase the baud rate of our HF link are investigated. These techniques are referred to as data compression.

The purpose of data compression is to allow the information through a given amount of bandwidth to be increased. This is done by maximizing the information content of each bit transmitted through the medium. Several

compression algorithms are in use which attempt to reduce the size of the message and thus allow more efficient use of the communication links. This section discusses criteria and use of data compression mechanisms and a proposition is made as to which algorithm is better to use here.

With data compression algorithms we can obtain better results in our HF environment. If a compression of 3:1 can be obtained, then the transmitted content of the data rate is tripled over the initial baud rate. So, a circuit operating at 2400 baud will transfer data at 7200 baud.

There also exists a disadvantage with data compressions when they are sent on end-to-end encrypted circuits. Using encryption data are presented to the compressor as a sequence of random bits except the header in the packet, thus the compressor will not be effective. Also, compression is not able to work when the data are not textual, not containing recognizable characters. It would be noted that even if no compression takes place, the data are not damaged in the system.

1. Types of compression implementations

There are two compression implementations: dynamic and static. Dynamic is the type of compression where the coding scheme is contained in the transmitted message. The disadvantage with this method is that if the coding scheme is damaged, the message will never be decompressed.

Static systems include the coding scheme within the compressor itself. This system does not have the disadvantages of the dynamic scheme. For robustness reasons, static systems are best for our HF system or any other system which is operated in a military environment.

Another complementary alternative to link compression is end-to-end compression. This means that compression is takes place at the application layer where a suitable algorithm can be used for the particular data. These two compression algorithms, link compression and end-to-end compression, are complementaries and our system can gain benefits from both of them.

2. SQueeze/UnsQueeze Compression

This method belongs to the dynamic type described above, and is designed for microcomputer communications to cut down on telephone connect time. It generally has a compression efficiency of 1.8:1 or 2:1. The squeeze scheme creates a statistical frequency table by counting characters in a message. As a result, the most frequent characters are coded with a short bit pattern while less frequent characters are coded with longer bit patterns. Then the message is compressed by substituting for the characters, the bit patterns.

3. Front End Compression

Front end compression is a technique whereby records with like beginnings are compressed. This is used more

frequently in database management system for index compression than in data communications applications. For that reason, it is of little use as a link encoding algorithm and is not discussed further.

4. Tokenization or Common Word Compression

Tokenization, as it is generally called, is a computerized method of brevity codes and belongs to the static type described above. It is a technique whereby commonly used words or phrases can be represented by tokens that are shorter. For example, in a hospital application common words like patient, insurance, bill, x-ray, doctor and nurse can each be represented by shorter bit forms. In the military there is a great number of words or phrases which are represented by brevity codes. Additionally, tokenization schemes can effectively operate at the logical link level on bit streams passing through the compressor, while squeeze/unsqueeze methods operate on a complete file in a batch. At the receiver, the algorithm is reversed, the token is replaced with the original bit sequence.

A commercially available tokenization scheme is capable of data compression in the 3:1 to 4:1 range for text files, a range that makes it quite attractive. Also, there are several other advantages which lead to the selection of tokenization. Some of them are:

First, tokenization schemes provide a quite high efficiency for data sequences including predictable

141

structures. These efficiencies of 3:1 compression are very attractive to our narrow bandwidth HF environment.

Second, tokenization is very easy to perform on a data stream, since it includes the coding scheme in the compressor.

Third, tokenization can be applied to several kinds of data, as graphic images which include a large amount of white space, data that can be compressed efficiently. The problem with this method is the inability to compress an encrypted end-to-end bit stream.

The last advantage of tokenization is that it belongs to the static type. As we mentioned above this type includes a lookup table imbedded in the transmitter and receiver. This table cannot be lost during the data transmission as can occur with the dynamic type. If during the propagation an error occurs in the data, it will be confined to the phrase that was tokenized and will not propagate to the entire packet.

The result of this section is that tokenization schemes are the most effective data compression techniques and a tokenizing data compressor is envisioned in the link transmitters and receivers.

VI. AN APPLICATION IN HELLENIC NAVY-CONCLUSION

A. GENERAL

The main body of this thesis ended with the previous chapter. During the main body, an architecture was given for a ship-shore packet switching communications network. The last three layers of the ISO reference model, Physical link, Data link and network link were described and applied to sea service communications.

In this chapter, we are going to examine the architecture issues of a ship-shore packet switching communications network to see if they can be applied in the Hellenic Navy.

First, a brief introduction will be presented to describe Hellas and the Hellenic Navy. Then, an examination of a Local Area Network applicable especially to the Hellenic Navy will be performed.

This chapter will close with an examination of this communication system architecture in the Hellenic Navy.

B. HELLAS AND THE HELLLENIC NAVY

Hellas is composed of the southern tip of the Balkan Peninsula and an archipelago of 3100 islands spread around the mainland into the Agean and Ionian seas in the eastern Mediterranean.

Hellas is a very old land with a rich history spanning over 5000 years. Its history is full of struggles for freedom and independence. Our intention is not to narrate the Hellenic history here, but to show that Hellas occupies an important location. Hellenic history is another topic, and the excited learner must run and read from any of the many volumes which exist in every library.

As we mentioned above, Hellas consists of a mainland and about 3100 island spread within its two seas. So, Hellas is an island region and needs strong naval protection. A map of Hellas is shown in Figure 6.1. A Navy protecting an island region such as Hellas must be very well organized. One very important issue affecting the ability to protect Hellas is that of communications. This issue affects two vital areas. The first area of concern is communication between island naval stations. The other area of concern is communication between operational ships.

To solve the first problem, communications between islands' naval stations, a well organized Local Area Network is required. For the next problem, communications between operational ships, an application of this thesis architecture must be implemented.

During the last few years, Hellas has been supplied with brand new ships, such as frigates, submarines, missile patrol boats etc. These units were also equipped with synchronous electronic equipment such as computerized weapon
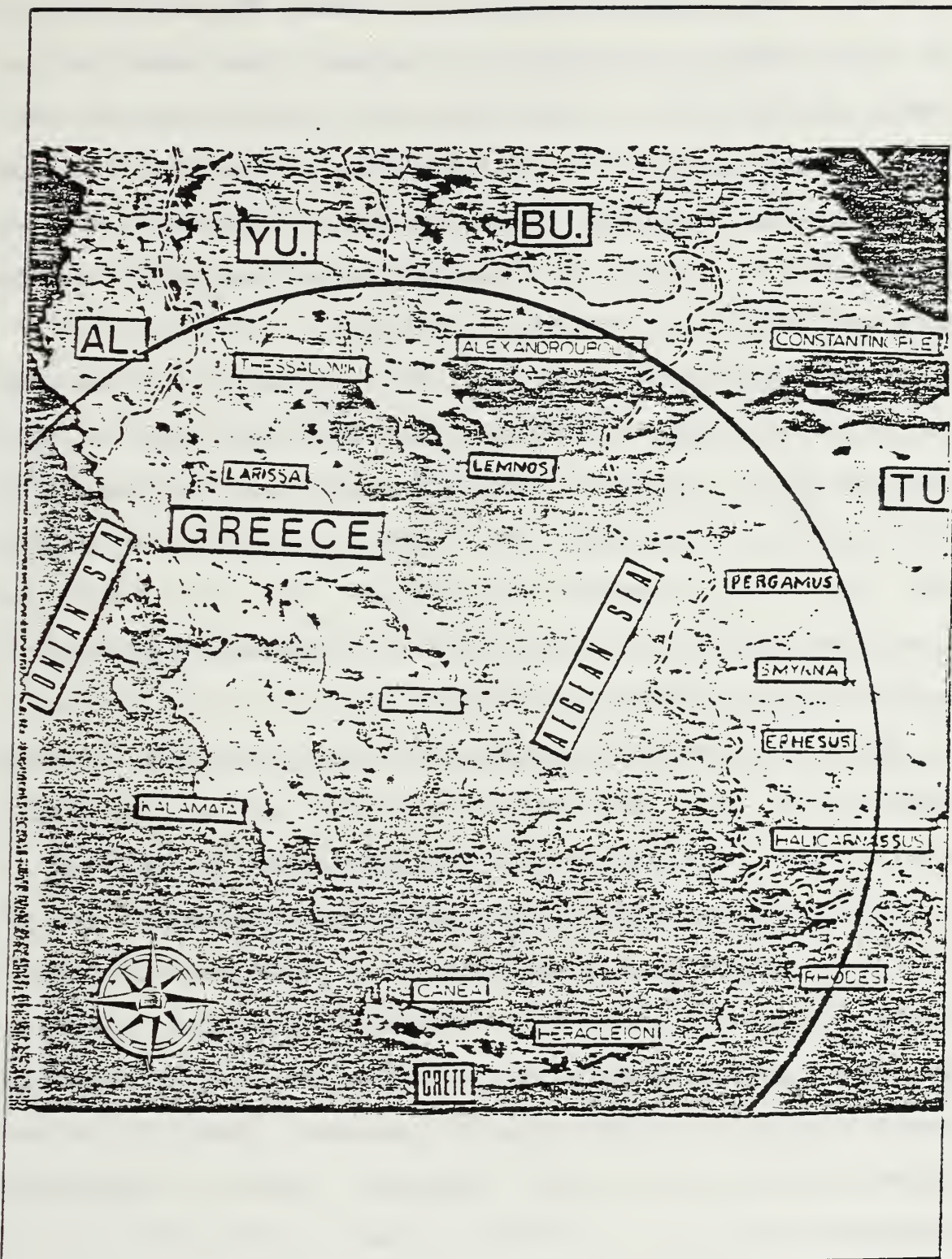
Figure 6.1   Map of Present Hellas.

systems, communications systems etc. Thus, the Hellenic navy is sufficiently prepared to upgrade its communication capability by adding a data computer system. Besides that, this thesis prepared an architecture of ship-shore packet switching communications which provides a framework able to accommodate a variety of physical layer equipment, as has been mentioned in the previous chapter.

Also, communications is the most important subject in operational purposes [Ref. 11]. The past has taught us that many important records of military operations have been lost due to lack of communications. Today, more than ever, Hellas must join the computer revolution in the area of communications if it is to be successful in future operational and defense activities.

There is a reasonable question to ask here: What are the benefits of this application? In addition to this thesis architecture, an engineering study must take place first to solve all engineering problems. After that the answer to the above question will be ascertainable. To derive concrete benefits will require future research if the Hellenic Navy decides to implement this thesis architecture. This research should consist of a "cost-benefit analysis" [Ref. 12] of the implementation of sea service packet switching communications.

C. HELLENIC NAVY LOCAL AREA NETWORK (HN/LAN)

Our intention, from the beginning was for this thesis to have universal application. Therefore, the application of this architecture in a HN/LAN will not be developed here. If it was developed, it would dilute the universal applicability of the architecture.

Much research on Local Area Networks (LANs) and many standards have already been developed. A well organized, and still under continuous development network is the Advanced Research Projects Agency Network (ARPANET). More details about the ARPANET approach to protocols are provided in Appendix C.

Nevertheless, during this chapter the intention will be to explain some different ways to connect the islands' Naval stations. Following are the advantages and disadvantages of each one:

1. Twisted Pair and Cable

The transmission medium is the physical path between transmitter and receiver in a communications network.

We can use sink wires to connect the islands Naval bases. By far the most common transmission medium, for both analog and digital data, is that of twisted pair. A twisted pair consists of two insulated wires arranged in a spiral pattern. The material usually used for the wires is copper or steel coated by copper. Copper is used to provide conductivity; while steel is used for strength. A twisted

147

wire pair acts as a full duplex communication link between two stations. Usually a number of wire pairs are bundled together to form a cable by wrapping them in a plastic protective sheath.

Twisted pairs can easily provide data transmission over a distance of 15 Km or more, transmitting both analog and digital signals. For analog signals, amplifiers are required about every 5 to 6 Km. For digital signals, repeaters are required every 2 or 3 Km. The most common use of wire pair is for analog transmission of voice. Digital data may be also transmitted over an analog voice channel using a modem.

Noise immunity is achieved by proper shielding and by using different twist lengths for nearby pairs in a bundle. These result in effective measures for wavelengths much greater then the separation of pairs in the cable. The twisted pair is cheap compared with other transmission media in terms of cost per foot. However, its installation cost is expensive due to connection limitations.[Ref. 5]

   2.   Coaxial Cable

Another transmission medium for local networks is coaxial cable. There are many kinds of coaxial cables specified in terms of their resistance in Ωhms (Ω). Most currently in use for local applications are: 75Ω and 50Ω cables. The first one is called broadband and is used for analog signaling with Frequency Division Multiplexing (FDM)

and for digital and analog signaling without FDM. The second
is called baseband and is only used for digital signaling.

The coaxial cable consists of two conductors. The
outer cylindrical conductor which surrounds an inner wire
conductor. For these two conductors, the inner can be either
solid or stranded, the outer can be either solid or braided.
The inner conductor is held in place by either regularly
spaced insulating rings or solid dielectric. The outer
conductor is covered with a protective shield. Its diameter
is 0.4 to 1 inch.

With this kind of transmissions medium it is
possible to accomplish maximum distances, in a typical
baseband cable, of a few kilometers, and with broadband
cables, a range of tens of kilometers. The difference in
distances is due to relative signal integrity of analog and
digital signals. In the case for high-speed data
transmission (50 Mbps), the distance is limited to about
1 Km for both digital and analog signals.

Noise immunity for coaxial cables depends on the
application and implementation, but in general, coaxial
cables are superior to twisted wire pairs, especially for
higher frequencies. The installation cost is also less than
twisted wire pairs.[Ref. 5]

3. <u>Fiber Optics and Optical Cable</u>

Fiber optics is one of the most exciting
development, of our era. It is replacing little by little

all the transmission media which exist in the realm of local networks.

Optical fiber can be constructed from various glasses and plastic, and its final form is a very thin string (50 to 100 μm), very flexible and capable of conducting an optical ray. Fiber optics can be classified in three categories depending on the losses. The lowest losses have been obtained using fibers of ultrapure fused silica. This kind of fiber optics is difficult to manufacture. In the second category belong fiber optics of multicomponent glasses. These have intermediate losses, are manufactured economically and provide good performance. The third category consists of fiber optics constructed of various plastics. Plastic fiber is even less costly and can be used for short-haul links for which moderately high losses are acceptable.

An optical fiber, glass or plastic with a high index of refraction, is surrounded by a cladding layer. This layer is constructed of material with slightly lower index of refraction. So, the fiber is isolated and cross talk is prevented with adjacent fibers.

A bundle of fibers consists of a fiber optic cable which sometimes is reinforced with a steel core. Another alternative to fiber optic cable is a stacked ribbon cable. This consists of a stack if flat ribbons each one with a single row of fibers.

150

Recently, fiber optics technology has accomplished transmissions over distances of 6 to 8 Km without repeaters. The most common use of optical fiber is for point-to-point links. There are also experimental multipoint systems, but they are too expensive for practical use.

Noise immunity is not required for fiber optics. They are little affected by electromagnetic interference or noise. This is also a characteristic of fiber optics that permits high data rates (50 Mbps) over long distance and provides excellent security.

Currently, the fiber optics transmission medium is more expensive compared with twisted wire pair and coaxial cable in terms of cost per foot and required components (transmitters, receivers, connectors). But, engineering advances should reduce the cost of fiber optics to be competitive with the other media (twisted pair and coaxial cable).[Ref. 5]

4. Line-of-Sight Media

In this section we will examine three transmission media which are used for transmitting electromagnetic waves through the atmosphere. These include infrared, laser and microwave. All these techniques have a unique characteristic, they require a line-of-sight path between transmitter and receiver. Since these techniques have high frequency ranges they operate at every high data rates.

151

Experimental systems for short links can transmit data rates of several megabits per second [Ref. 5].

In the rest of this section we will describe the characteristics and differences for each technique.

The first technique, infrared link, consists of a pair of transmitter/receivers or an embodied transceiver that modulates noncoherent infrared light. These devices must be within line-of-sight installed on either a roof top or in a tall building with data transmitted through an adjacent exterior window. The system can be installed in just a few days. This technique is highly directional, extremely difficult to intercept, inject data, or to jam, excellent maintenance and low cost. [Ref.5]

The second one, laser link, also consists of a pair of transmitter/receivers or an embodied transceiver using coherent high modulation. The properties of this technique are easy installation in just a couple of days, data rate 1-3 Mbps range, excellent maintenance and low cost. This system emits low-level radiation, so it must be properly shielded. [Ref. 5]

The last, microwave link, is a system with less sensitivity to environmental interference, such as rain and fog, than infrared and laser links. System installation is easy, as with infrared and laser, in just a week. This system has two disadvantages which make it different from the other two systems. First microwave, is not directional.

This requires microwave transceivers to be mounted in the external environment. Also, a security problem exist due to data eavesdropping, injection, or jamming. This system is has little and a low cost. [Ref. 5]

5. Choice of Transmission Medium

The main question which arises in the Hellenic Navy Local Area Network (HN/LAN) is "of the transmission mediums, which one is best suited for use by the Hellenic Navy?". The answer is that there is no one specific transmission medium proposed which is markedly better with the HN/LAN. Since Hellenic islands are peculiar and unique with factors such as distance, line-of-sight path etc, a combination of the above described media will be used in the HN/LAN.

The choice of transmission medium is determined by a number of factors. These factors are examined in the rest of this section and include: [Ref. 5].

* Capacity. This is provided to support local network traffic.

* Reliability. To meet availability requirements.

* Types of data supported. These types of data are tailored to each application.

* Environmental scope. This is to provide service over the range of environments required.

Under these conditions, it will be worth while to make a few observations about transmission media.

Twisted pair is an expensive but well understood medium. Compared with coaxial cable, the band-width is

153

limited. It is likely to be most effective for low traffic, local network installation.

Coaxial cable is more expensive than the twisted pair but has greater capacity. Coaxial cable excels when there are many devices and a reasonable amount of traffic. For the broad range of local network requirements, and with the exception of terminal-intensive systems, coaxial cable is the transmission medium of choice.

Fiber optics are most applicable for point-to-point communications. Multipoint fiber optics are in experimental stage. However, when the cost of multiple fiber cable comes down, its advantages of low noise susceptibility, low loss, small size, and light weight [Ref. 5] will make it an attractive transmission medium for local network requirements.

The line-of-sight media are well suited to specific cases of local networks which fullfill the properties which were described above. They are a good choice for point-to-point links in a range covered by line-of-sight media techniques.

D. COMMUNICATIONS BETWEEN OPERATIONAL SHIPS

This section includes the manner with which the operational ships can communicate with the communication stations for receiving orders. This communication consists of packet switching transmission, a good application of this

154

thesis. The result is that the best approach is half duplex. This can be accomplished by using a frequency bandwidth or via satellite transmissions. This is illustrated in Figure 6.2.

All the problems associated with this communication system can be solved by engineering processes. By that, we mean communications stations and operational ships can readjust their physical level equipment to implement this communication system. The only problem in this case is to find out if the required circular dish antenna of the satellite to cover the Hellenic region is feasible. This is primarily required for avoiding, as much as possible, interference from other communications stations. The rest of this section and the conclusion of this thesis will be to determine the feasibility of the satellite circular antenna.

The formulas which will be presented in the sequence are from class notes of course EC 3750 offered by Major Tom Brown in summer 1986 quarter.

The problem which arises is as follow: A communication satellite is planned to orbit the earth at an altitude of 35,784 Kilometers. The satellite will be moving with respect to the Earth's surface, so a pointing mechanism on the satellite will keep its circular dish antenna pointed to cover Hellas's area with a circular region of radius 250 nautical miles. Tactical satellite communicatins is operated with frequency 7.5-8.5 GHZ, so the satellite down link will
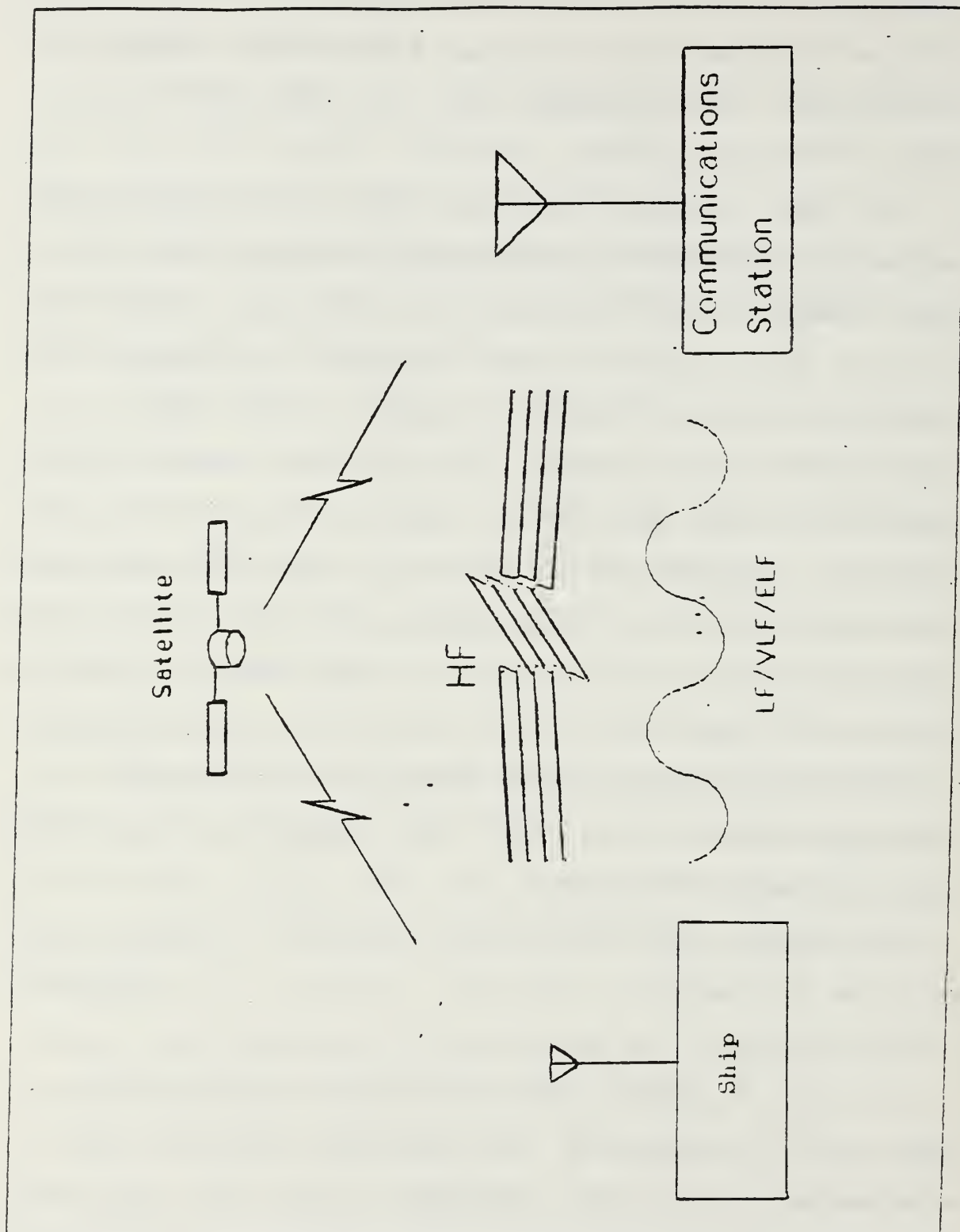
155

Figure 6.2   Ship-Shore Communications Systems.

be operated with a carrier frequency (fᶜ) of 8.0 GHZ. This problem is illustrated in Figure 6.3.
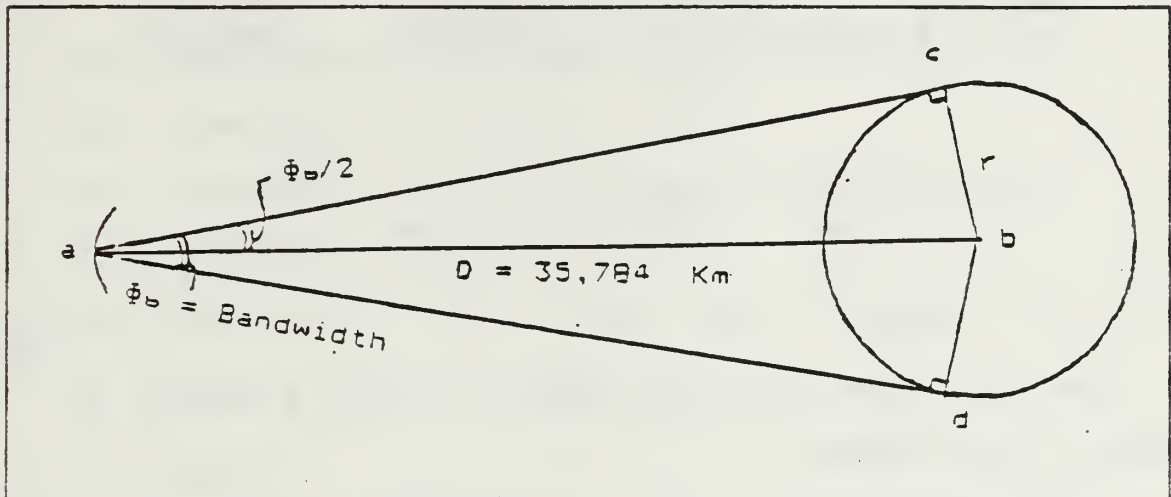
Figure 6.3   Satellite Communication Problem.

From the triangle abc we observe that

$$r = D*\sin\frac{\Phi b}{2} \qquad (6\text{-}1.)$$

where

r = Hellas's circular region radius

D = Satellite altitude

Φb = Beamwidth, the angle to cover Hellas's circular

region from the satellite

by rearranging this formula, we have

$$\frac{r}{h} = \sin\frac{\Phi b}{2} \qquad or \qquad \frac{\Phi b}{2} = a = \sin^{-1}\frac{r}{h}$$

157

if we substitute the known values, we have

$$\frac{\Phi b}{2} = a = \sin^{-1}\frac{463.25}{35,784} = 0.012945 \qquad \text{radians}$$

$$\text{or} \qquad \frac{\Phi b}{2} = a = 0.74^0$$

The field view, the solid angle to cover a region, is given by the formula

$$\Omega fv = 2\pi\left(1-\cos\frac{\Phi b}{2}\right) \qquad (6\text{-}2)$$

if we substitute the known values, we find that the required field of view to cover Hellenic's circular region is

$$\Omega fv = 2*3.14\left(1-\cos 0.012945\right)$$

$$\text{or} \qquad \Omega fv = 526.26*10^{-6} \qquad \text{steradians}$$

We need to determine the required radius of the satellite circular dish antenna, so we have to calculate first the maximum available satellite antenna gain, to assure receipt of a signal at the earth station. This maximum satellite antenna gain is given by the formulas

$$g = \frac{4\pi}{\Omega fv} \quad \text{(6-3)} \qquad \text{or} \qquad g = \frac{4\pi}{\lambda^2} * A \quad \text{(6-4)}$$

where

   g = satellite antenna gain

   λ = wavelength in meters

   A = physical area of the satellite circular dish

        antenna

if we substitute the known values into formula (6-3), we
have

$$g = \frac{4*3.14}{526.26*10^{-6}} = 23866.53 \qquad \text{or} \qquad g = 43.78 \quad db$$

by rearranging formula (6-4), we have

$$A = \frac{g\lambda^2}{4\pi} \quad \text{(6-5)}$$

   Also, the wavelength is given by the formula

$$\lambda = \frac{c}{f} \quad \text{(6-6)}$$

where

   c = velocity of wave propagation in free space, $3*10^8$

       meters per second (m/s)

   f = frequency in hertz

159

by substituting equation (6-6) to (6-5), we have

$$A = \frac{g\left(\dfrac{c}{f}\right)^2}{4\pi} \qquad\qquad (6\text{-}7)$$

if we substitute the known values to this formula, we have

$$A = \frac{104.378 * \left(\dfrac{3*10^8}{8*10^9}\right)^2}{4*3.14} \qquad \text{or} \qquad A = 2.67 \quad m^2$$

but A , the physical area, is given by the formula

$$A = \pi R^2 \qquad\qquad (6\text{-}8)$$

where

    R = radius of satellite circular dish antenna

by rearranging this formula, we receive

$$R^2 = \frac{A}{\pi} \qquad \text{or} \qquad R = \sqrt{\frac{A}{\pi}}$$

if we substitute the known values into this formula, we have
the radius of the satellite circular dish antenna

160

$$R = \sqrt{\frac{2.67}{3.14}} = 0.92 \quad m \qquad or \qquad R = 3.04 \quad feet$$

As a result, the calculations determine that the required circular dish satellite antenna to cover Hellenic circular region of a radius 250 nautical miles or 463.25 Kilometers has a radius of 3.04 feet or 6.08 feet diameter, which is a feasible dimension.

APPENDIX A

DATAGRAM AND VIRTUAL CIRCUITS

There are two basic kinds of "service" in a packet switching network, determined by the way the packets arrive at their destination. These two kinds are: Datagram service, and Virtual Circuit service.

1. DATAGRAM APPROACH

In the datagram approach, each packet is treated independently, just as each message is treated independently in a message-switching network. That means, each packet of a message finds its own path through the network according to the current information available at the nodes visited, and independently of the other packets of the same message. There is not any provided relationship between the order in which one node enters packets into the network, which are referred to as "datagrams", and the order in which these same datagrams arrive at their destination. The use of this approach requires information for its routing be included in each datagram. Therefore, each packet will typically contain in its header the following information: The destination, the message to which it belongs, packet number, and any other information required by the particular routing scheme implemented.

162

2. VIRTUAL CIRCUIT APPROACH

In the virtual circuit approach, a logical connection is established before any packets are sent. That means, a particular path is set up when a session is initiated and maintained during the life of the session. So, the order in which the packets are entered into the network is the same order in which they arrive at their destination. This is assumed by requiring that all the packets of a message follow the same path as the first packet. Therefore, each packet only needs in its header an identification of the virtual circuit to which it belongs, and the different nodes will automatically route it through the links that correspond to the virtual circuit.

So the main characteristic of the virtual circuit approach is that a path between stations is set up before data transfer. Note that this does not mean that there is a dedicated path, as in circuit switching. A packet is still buffered at each node and queued for output over a line. That means more than one virtual circuit may simultaneously include the same link as part of the route for its packets and thus share the use of that link. Another important difference is with a link failure. Then a packet may be routed through alternative routes and contact is not lost as would occur with line switching.

Each virtual circuit requires an explicit establishment procedure which generally is done by the first packet of a

message or a request-to-send (RTS) packet. This procedure also establishes the route, and is followed by a data transfer and a shutdown procedure. Once the circuit has bee established the packets are not required to carry their destination, since it was defined during set up. This allows the packet to carry more data. Virtual circuits appear to the end user as if they were dedicated lines; however, within the network many different virtual circuits share the same communication links.

Virtual circuit routing is generally used in practice, although there are many interesting intermediate positions between them. If two stations wish to exchange data over an extended period of time, there are certain advantages to virtual circuits. They all have to do with relieving the stations of unnecessary communications processing functions. A virtual circuit facility may provide a number of services including sequencing, error control and flow control, services which were described at length during this thesis.

APPENDIX B

THE X.25 PROTOCOL

The main offered contribution of the x.25 protocol is a set of functions that are under the control of the user computer. This set of functions between user-network interfaces is shown in Table II [Ref. 2]. Also, Table II categorizes these functions by three protocol levels for controlling and implementing purposes.

TABLE II

FUNCTIONS AT THE USER-NETWORK INTERFACE [Ref. 2]

Level 1	Synchronization
Level 2	Error detection
2	Correction by retransmission
2	Transparency
Level 3	Sequencing
3	Flow control
3	Multiplexing
3	Call set-up and clearing
3	Provision for network internetting
3	Logical in-band signaling
3	Logical out-of-band signaling

165

The networks, under X.25 standards, have a high probability of successful transmission. That means, these networks insure two basic implementations. First, an alternative routing exists for network failures, and second a method exists for controlling network congestion. Beside these basic implementations, the network is required to implement the fundamental switching functions and to insure the proper sequencing of packets delivered and to account for packets actually delivered.

This appendix includes the general structure of the call-request packet and the structure of the user data packet.

1. STRUCTURE OF THE CALL-REQUEST PACKET

Current implementations of the X.25 compliant network operation are virtual circuit, which we examined in Appendix A. Also, the 1980 version of X.25 now includes standards for datagram mode of operation. Packets are controlled within the network to insure that they are delivered in sequence, but the user must place a sequential number in each packet on a particular logical channel.

The general structure of the call-request packet is illustrated in Figure B.1. This packet consists of a sequence of fields. Each field has either a predefined or a specified length, and a set of agreed-on codings. In the
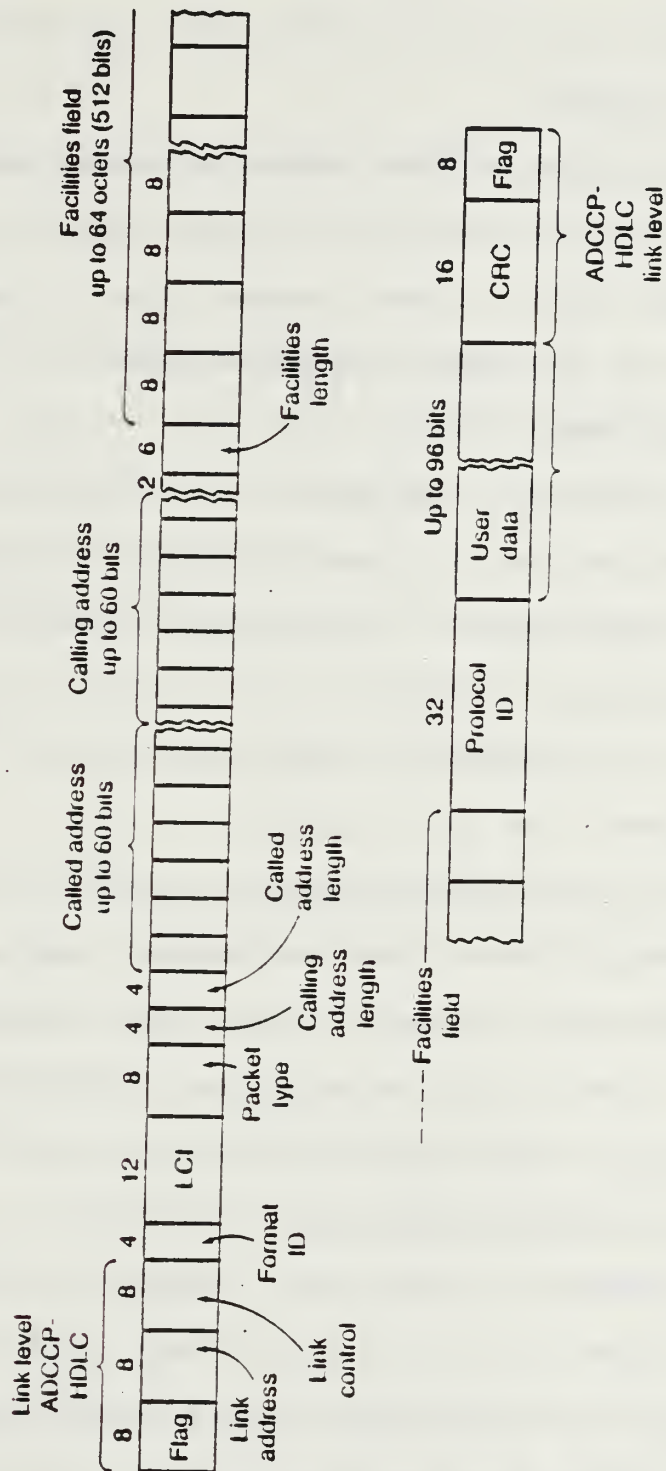
Figure B.1   Call-Request Packet Structure.

167

following the functions of the various packet fields are shown. [Ref. 2]

    a. **Flag (8 bits)**

        The beginning and the end of a packet are denoted by the binary number 01111110. In the case of successive packets a single flag is used between them to denote the end of one packet and the beginning of the next.

    b. **Link Address (8 bits)**

        This address is limited to the devices at each end of the connecting link between the data terminal equipment (DTE) and the data circuit-terminating equipment (DCE).

    c. **Link Control (8 bits)**

        This is primarily used for error control and correction between the DTE and DCE.

    d. **Format Identifier (4 bits)**

        The format identifier designates the nature of the packet that follows, such as a new call request, a data packet or a previously established call and defines the sequence numbering range (8 or 128).

    e. **Logical Channel Identifier (12 bits)**

        This defines the logical channel number for this data call. It can take any value from zero to 4095. This permits a single user to control up to 4096 individual data flows over a single line simultaneously.

f.   Packet type (8 bits)

This defines the function and the content of this packet.

g.   Calling address length (4 bits)

This defines the length of the calling party address.

h.   Called address Length (4 bits)

This defines the length of the called party address. Like the calling address length this consists of a binary representation of a number from zero to 15 that defines the size of the address contained in a subsequent field.

i.   Called Address (up to 60 bits)

This field includes the address of the destination party.

j.   Calling address (up to 60 bits)

This field includes the network address of the calling party. Like the called address, the length of this field is determined by a previous field.

k.   Facilities Length (up to 512 bits)

This is a binary representation of a number from zero to 63, and indicates the length, in 8-bit octets, of the following facilities field.

l.   Facilities Field (up to 512 bits)

This field provides for a large number of optional network facilities, such as reverse charging, a closed user group, one-way connections and the like.

169

m. Protocol Identifier (32 bits)

This field can be used for certain user-level protocol features. These include, the user identification and log-on procedure for initiating a new connection.

n. User Data (up to 96 bits)

In the call-request packet, the user can transmits up to 96 bits of data. This data may be, for instance, the user's password.

o. Cyclic Redundancy Check (16 bits)

This is a method for error detection applied to all bits from the flag up to the end of the user data field.

p. Flag (8 bits)

The binary number, 01111110, which denotes the end of this particular packet.

2. STRUCTURE OF THE DATA TRANSFER PACKET

Once the call has been established, the data transmission takes place. This is done by using an abbreviated version of the data packet structure as illustrated in Figure B.2. The overhead required with the data packets is considerably less than that required for a call-request packet, thereby permitting efficient use of the circuit. In this case the necessary information for routing the packets through the network is stored in the switches, referenced to the source and the current logical channel identifier.

Again, each packet consists of a sequence of fields. In the following the functions of the various packet fields are shown [Ref. 2].
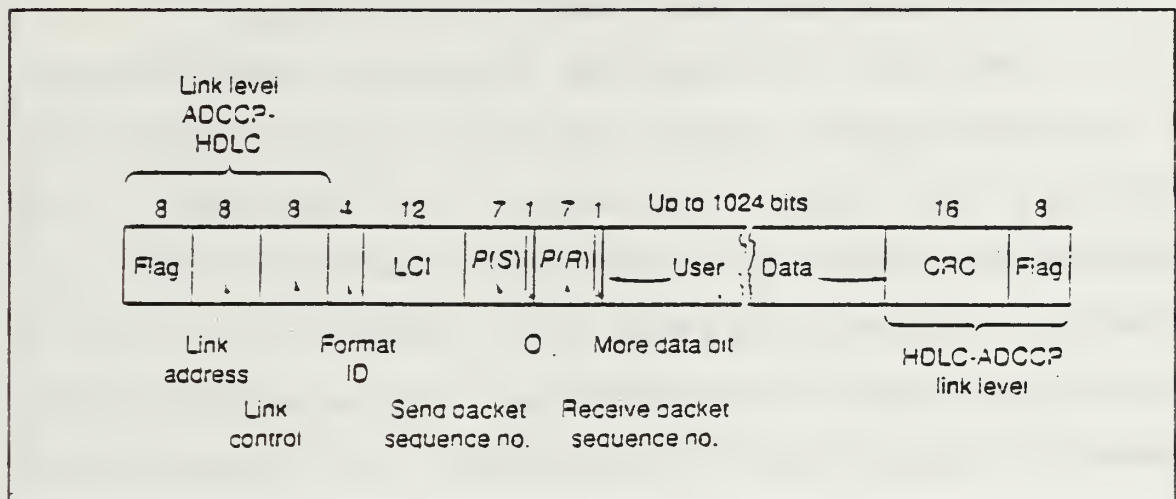

Figure B.2   Data Packet Structure.

a. Flag (8 bits)

The sequence 01111110 denotes the beginning of the packet.

b. Link Address (8 bits)

This address is limited to the devices at each end of the connecting link between DTE and DCE. the network address is contained in the packet header.

c. Link Control (8 bits)

This is primarily used for error control the DTE and the DCE.

d. Format Identifier (4 bits)

The format identifier defines the nature of the packet and it would be coded to indicate a data packet.

171

e.   Logical Channel identifier (12 bits)

This logical channel identifier refers to the particular channel assigned during the call set-up process.

f.   Send Packet Sequence Number (3 or 7 bits)

This field includes the sequential number assigned to each successive packet on this logical channel. The existing counter varies from zero to 7 or from zero to 127 depending on the coding in the format identifier field. Also the size of this field depends on two factors. The first is the network speed of operation and the second the maximum number of packets which is permitted for a given user to have outstanding in the network.

g.   Receive Packet Sequence Number (7 bits)

This field includes the number of the last packet successfully received on the channel connection. The network switches inform the user with the sequence number of the last packet successfully received and acknowledged by the other user on the connection. It is the main method of acknowledging data.

h.   More Data Bit (1 bit)

This field can only have two values, zero and one. It gets a zero if this is an acknowledgment only, and no more data is desired at this time. It gets a one if the user is prepared to receive more data.

i. User Data Field (up to 1024 bits)

This is the transparent data field for up to 1024 bits or 128 data characters.

j. Cyclic Redundancy Check (16 bits)

This is a method for error detection applied to all bits from the flag up to the end of the user data field.

k. Flag (8 bits)

The sequence 01111110 denotes the end of the packet. The last two sections of this Appendix consist the basic packets format. A number of special purpose packets can be derived from these by using a combination of the format identifier field, packet type identifier, and address fields. Thus, the combination of packets can handle a variety of anomalous network conditions, for example, network or user-initiated restarts or interrupts, clear connection requests, and signaling inquiries and responses.

It is important to emphasize that this standard (X.25) addresses the interface between the user and the network. The structure of the packets internal to the network are up to the network designer and are not specified by the X.25 standard. [Ref. 2]

APPENDIX C

THE ARPANET APPROACH TO PROTOCOLS

The word ARPANET is the abbreviation of the Advanced Research Projects Agency Network, which is an operational digital network within the U.S. Department of Defense. This network is generally credited with making packet switching a practical reality. Also, it implements its original concept as a resource-sharing network among many computer centers. It is now very much representative of advanced research in data communications techniques and distributed data processing. It is used for a wide range of research and development in U.S.A and in some countries in Europe.

1. STRUCTURE OF THE NETWORK

The ARPANET consists of two kinds of switches. The first kind is known as the Interface Message Processor (IMP) and is designed to operate only with computers. The second kind is called as Terminal Interface message Processor (TIP) and is able to operate with a combination of computers and individual user terminals. [Ref. 2]

The communication between host computers is achieved via network messages up to 8159 bits in length. In this length, the first 96 bits of a message are used to specify the destination address and handling information. This is called

174

the message leader. The leader information uniquely specifies a connection between the source and the destination hosts. A message identification number is used to manage and control the message through the network until the message delivery is confirmed back to the source host. The nodes in the network are programmed to receive and forward messages to the next nodes, with end-to-end delays up to about one-quarter second. In the data packet there exists a packet header in addition to the user data. This packet header consists of the address information and network control information required to protect the flow of the packet through the network. The address information is the same as that included in the message header. [Ref. 2]

2. MESSAGE HANDLING PROCEDURE

An interesting part of the ARPANET is the message handling procedure. This procedure is illustrated in Figure C.1. This figure represents two host computers exchanging messages through an originating packet switch, a tandem switch, and a destination packet switch. Message segments can arrive at the originating packet switch via either a single high-speed local transfer or a block-by-block transfer over a data-link controlled access line between the host and the switch. Blocks of data are usually transmitted from the host to the switch under control of the data-link level (layer 2) of the protocol hierarchy.[Ref. 2]
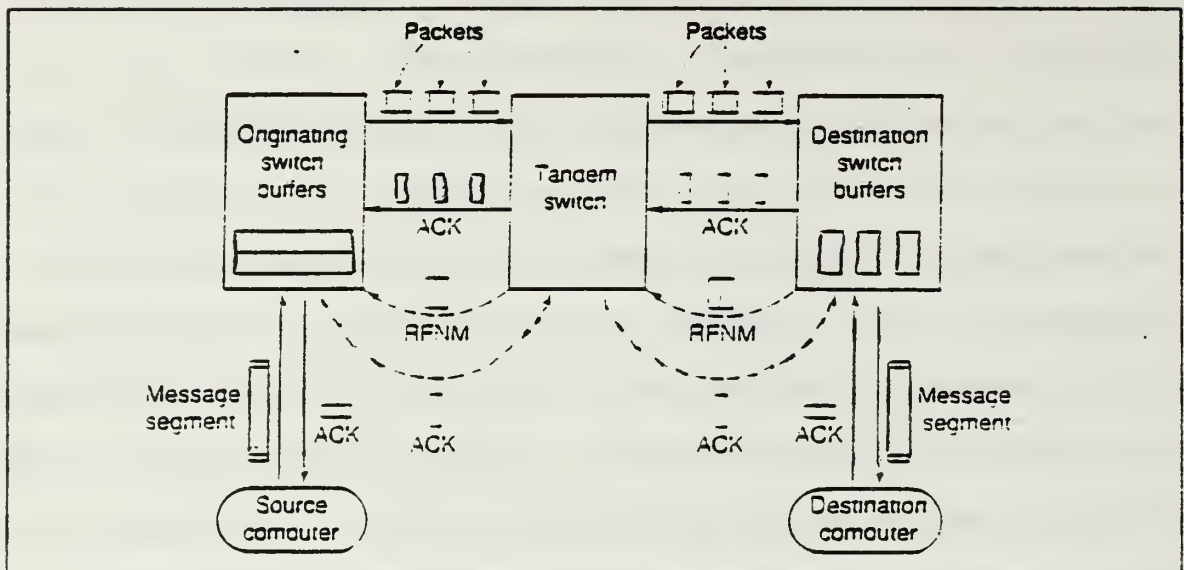
Figure C.1   Operational Model of an ARPANET.

The information field included in these blocks may or may not be the same as the information field included in the packets. In any case, the message segment, after arriving at the originating switch is temporarily stored in its buffers. This causes the originating switch to initiate several actions at the network and transport layers, as well as at the switch-to-switch protocol levels.

The new message flow generates the entry of information into a "Pending Leader Table (PLT)", which the originating switch uses to create the packet headers for the individual packets of the message from the user-supplied leader information. Simultaneously the originating switch requests the destination switch to allocate a set of buffers for reassembling the individual packets into the complete message segment. The allocation request (RECALL) short control/information packet transits the network rapidly and

176

indicates to the originating switch the availability of destination buffers. The buffer availability is designated by returning an allocation (ALL) control message from the destination switch to the origination switch. Then the transmission of the individual packets composing the message is initiated.

The packets composing the message can arrive at the destination switch in a different order than they are transmitted from the originating switch. This is caused by network operation that includes error detection, error correction, dynamic routing and other features that affect the end-to-end transmission. When the message is reassembled in the destination switch buffers, it is sent to the destination computer. In the sequence, the destination switch sends an acknowledgment in the form of a request for Next Message (RFNM), with an allocation for additional message segments. If no buffers are available, then a RFNM is sent without an allocation. [Ref. 9]

All the above describe the message handling procedure of the ARPANET occurring on an end-to-end basis. Each packet transmitted within the network is acknowledged on a link, switch-to-switch basis, to insure proper delivery and error-free transmission.

LIST OF REFERENCES

1. Buddenberg, Rex A., <u>Ship-Shore Packet Switched Communications System.</u> MS Thesis, Naval Postgraduate School, Monterey, California, June 1986.

2. Schiantarelli, Harry T., <u>Multiple Path Static Routing Protocols for Packet Switched Networks.</u> MS Thesis, Naval Postgraduate School, Monterey, California, Sept. 1983.

3. Rosner, Roy D., <u>Packet Switching, Tomorrow's Communications Today.</u> 1985.

4. Stallings, William, <u>Data and Computer Communications.</u> Colier, MacMilan, 1985.

5. Stallings, William, <u>Local Area Networks, An Introduction.</u> June 1978.

6. Stamper, David A., <u>Business Data Communications.</u> 1986.

7. Rossi, G. P., and Garavaglia, G., "Link Layer for co-operating Processes on a LAN with Enhanced communications Services," <u>Computer Communication Magazine</u>, v.10 number 3, June 1987.

8. Sloman, Morris, and Kramer, Jeff, <u>Distributed Systems and Computer Networks.</u> C.A.R., Hoare, 1987.

9. Katopodis, Thomas, <u>Spread Spectrum System: A Point of View between Technology and Management.</u> MS Thesis, Naval Postgraduate School, Monterey, California, Sept. 1986.

10. Davison, K. L., <u>The Ionosphere and HF Transmission.</u> Meteorology course notes, Summer Quarter, Naval Postgraduate School, Course MS 2400, 1986.

11. Ricci, Fred J., and Schutrer, Daniel, <u>U.S. Military communications, A C3I Force Multiplier</u>, 1986.

12. Littlechild, S. c., <u>Elements of Communications Economies.</u> 1979.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Department Chairman, Code 54 Department of Administrative Science Naval Postgraduate School Monterey, California 93943	1
4.	Professor Thomas J. Brown, Code 62Bb Department of Electrical and Computer Engineering Naval Postgraduate School Monterey, California 93943	1
5.	Professor Richard A. MacGonigal, Code 0305 Department of Administrative Science Naval Postgraduate School Monterey, California 93943	1
6.	Professor Dan C. Boger, Code 54Bo Department of Administrative Science Naval Postgraduate School Monterey, California 93943	1
7.	Hellenic Navy General Staff 2nd Branch, Education Department Stratopedan Papagou GR 155.61 - Holargos, GREECE	4
8.	CDR. Evagelos S. Agapiou L. Salaminos 204 Salamis - GREECE	6